

Universidad ORT Uruguay
Facultad de Ingeniería

Gestión del Riesgo basado en la Gestión del Conocimiento para empresas PyMEs de Uruguay

Entregado como requisito para la obtención del título de
Master en Ingeniería en Investigación

Lic. Sebastián Ayala - 96025

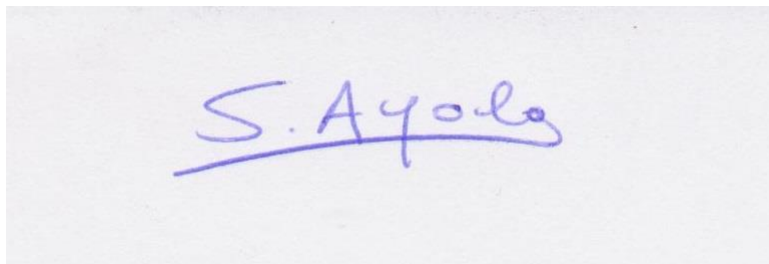
Tutor: Dra. Helena Garbarino

2016

Declaración de autoría

Yo, Sebastián Ayala, declaro que el trabajo que se presenta en esta obra es de mi propia mano. Puedo asegurar que:

- La obra fue producida en su totalidad mientras realizaba la Tesis Final de Maestría;
- Cuando he consultado el trabajo publicado por otros, lo he atribuido con claridad;
- Cuando he citado obras de otros, he indicado las fuentes. Con excepción de estas citas, la obra es enteramente mía;
- En la obra, he acusado recibo de las ayudas recibidas;
- Cuando la obra se basa en trabajo realizado conjuntamente con otros, he explicado claramente qué fue contribuido por otros, y qué fue contribuido por mí;
- Ninguna parte de este trabajo ha sido publicada previamente a su entrega, excepto donde se han realizado las aclaraciones correspondientes.

A photograph of a handwritten signature in blue ink on a light-colored surface. The signature reads "S. Ayala" and is underlined with a single horizontal stroke.

Sebastián Ayala

15/02/2016

Agradecimientos

Este trabajo no hubiera sido posible sin el apoyo y estímulo de muchas personas.

En primer término quiero agradecer a mi tutora la Dra. Helena Garbarino quien me dio la oportunidad de emprender este camino de investigación, desarrollo y conocimiento, brindándome todo su apoyo y orientación durante la realización de este trabajo.

También quiero agradecer a la Facultad de Ingeniería de la Universidad ORT, especialmente al Dr. Alvaro Tasistro, coordinador académico del Master por todo el apoyo brindado y a los profesores del Master que me permitieron encontrar un lugar para investigar.

Quiero incluir un especial agradecimiento al Sr. Gustavo Alves y a mis colegas por su apoyo, recomendaciones y críticas constructivas que permitieron la mejora continua del trabajo. También al Prof. Adrián Arnould quien contribuyó a través de traducciones al idioma inglés de artículos, libros así como trabajos y artículos que presente en conferencias durante la realización de este trabajo, lo que permitió la mejora en la calidad del mismo.

Quiero agradecer también a todas las organizaciones y personal de las mismas que colaboraron en el trabajo de campo aportando su conocimiento y experiencia para brindarme toda la información requerida de la mejor manera posible, atendíendome siempre con extrema corrección y deferencia.

Finalmente quiero agradecer a mi familia e infinitamente a mi esposa, Prof: Luciana Miranda y a mi hijo Dackwoon por su amor y apoyo permanente e incondicional, dedicando tiempo y recursos para que este proyecto familiar se pudiera culminar con el mejor de los resultados. Además un agradecimiento y reconocimiento especial a mis abuelos y padres, quienes me motivaron desde pequeño a investigar y aprender.

Abstract

La gestión del riesgo tiene un estrecho vínculo con la gestión del conocimiento. Si la organización gestiona adecuadamente el conocimiento e incorpora, preserva, disemina y utiliza el conocimiento de manera inteligente, tendrá la información necesaria para poder gerenciar adecuadamente el riesgo, previniendo, mitigando o eliminando el mismo en la organización.

Este trabajo realiza un relevamiento del estado del arte respecto al gobierno de TI, la gestión de riesgos y estrategias de diseño en gobierno de TI, así como en lo que respecta a la gestión del conocimiento y su vínculo con el gobierno de TI.

Dado que no se cuenta con trabajos que relacionen la gestión del conocimiento y la gestión del riesgo aplicado a empresas PyMEs, se plantea el presente trabajo dada la importancia de dichas empresas en nuestro país y el mundo.

Como resultado del estudio se crea un marco y se define un modelo de gestión del riesgo basado en la gestión del conocimiento, teniendo en cuenta su aplicabilidad a empresas PyMEs que presentan características especiales por su estructura y organización.

Para la validación de su aplicabilidad, se realiza un trabajo experimental relevando 2 empresas de Uruguay, logrando medir y determinar su nivel en base al modelo planteado, para el cual se definieron indicadores y sus medidas asociadas a cada nivel en el modelo.

Las empresas relevadas podrán identificar sus puntos de mejora respecto a la gestión de conocimiento aplicado a la gestión del riesgo, pudiendo ser relevadas luego de un período y valoradas nuevamente en base al modelo, determinando así el impacto de los cambios realizados.

Como trabajos futuros se plantea la posibilidad de elaborar un producto de software capaz de facilitar y automatizar la aplicación de este modelo, facilitando la evaluación y comparación de resultados.

Palabras clave

Español

Gestión del Conocimiento, Gestión del Riesgo, PyMEs, Modelo de Madurez, Marco de Gestión del riesgo.

Inglés

Knowledge Management, Risk Management, Maturity Model, Risk Management Framework

Glosario

Término	Definición
Acreditación	Declaración formal por una autoridad designada de aprobación de que un sistema está aprobado para operar en un modo particular de seguridad utilizando un conjunto prescrito de salvaguardas.
Activo	Cualquier cosa que tenga valor para la organización.
Amenaza	Capacidades, intenciones y métodos de ataque de los adversarios para aprovecharse, o cualquier circunstancia o evento con el potencial para causar daño a la información o al sistema.
Análisis de Riesgos	Proceso de identificar los riesgos de seguridad, determinar su magnitud e identificar las áreas que necesitan salvaguardas.
Argumento de Aseguramiento	Conjunto de demandas estructuradas de aseguramiento, soportados por la evidencia y el razonamiento, que demuestran claramente cómo se han satisfecho las necesidades de seguridad.
Aseguramiento	Grado de confianza de que las necesidades de conformidad de la información con leyes, normas, controles y objetivos tanto internos como externos se satisfacen.
Autenticidad	Propiedad que asegura que la identidad de un sujeto o recurso es el único demandado. La autenticidad se aplica a las entidades tales como usuarios, procesos, sistemas e información.
BCU	Banco Central del Uruguay. Fue creado en 1967. Tiene autonomía técnica, administrativa y financiera en los términos de la Constitución de la República y de la Carta Orgánica. Sus principales finalidades son la estabilidad de precios y la regulación y supervisión del sistema financiero y del sistema de pagos.
CAF	Corporación Andina de Fomento
CFI	Corporación Financiera Internacional. Entidad del Grupo del Banco Mundial que promueve el desarrollo sostenible del sector privado en mercados emergentes.
Cliente	Individuo u organización que es responsable de la aceptación del producto y de la autorización del pago a la organización del servicio / desarrollo.
Confidencialidad	Propiedad de que la información no está disponible o revelada a individuos, entidades o procesos no autorizados.

Término	Definición
Consistencia	Grado de uniformidad, estandarización y libertad a partir de la contradicción entre los documentos o partes de un sistema o componente.
Corporación	Es una entidad legal artificial, con personería jurídica bajo la ley, que tiene una entidad legal separada a pesar de que se compone de una variedad de otras entidades jurídicas y personas reales.
CRM	Sistemas de administración de relaciones con el cliente. Proveen información para coordinar todos los procesos de negocios que tratan con los clientes en ventas, marketing y servicios. [9]
Director	Miembro del más alto cuerpo de gobierno de una organización. Incluye propietarios, miembros del consejo, consejeros, socios, ejecutivos senior o similares y Oficiales Autorizados por el Gobierno.
Disponibilidad	Propiedad de estar accesible y utilizable bajo demanda por una entidad autorizada.
Eficacia	Propiedad de un sistema o producto que representa como de bien proporciona seguridad en el contexto de su utilización operativa propuesta o actual.
ERP	Sistemas de planificación de recursos empresariales. Integran los procesos de negocios de manufactura y producción, finanzas y contabilidad, ventas y marketing y recursos humanos en un solo sistema software.
Estrategia	Plan global de desarrollo de una organización que describe el uso eficaz de recursos en apoyo de la organización en sus actividades futuras. Comprende el establecimiento de los objetivos y la propuesta de iniciativas de actuación.
Evaluación	Evaluación por un equipo de profesionales entrenado para determinar el estado del proceso actual de las organizaciones, para determinar los problemas de alta prioridad relativos al proceso a los que se enfrenta una organización, y para obtener el soporte organizativo para la mejora del proceso.
Evidencia	Características mensurables directamente de un proceso y/o producto que representa la prueba objetiva y demostrable de que una actividad específica satisface un requisito especificado.

Término	Definición
Evidencia de Aseguramiento	Datos sobre los que se basa un juicio o conclusión sobre una demanda de aseguramiento. La evidencia puede consistir en la observación, los resultados de las pruebas, los resultados del análisis y las evaluaciones que proporcionan soporte para las demandas asociadas.
Gestión	El sistema de procesos y controles necesarios para alcanzar los objetivos estratégicos establecidos por los órganos de gobierno de la organización. La gestión está sujeta a la dirección marcada por la política y seguimiento establecidos a través de la gobernanza corporativa.
Exactitud	Propiedad de una representación de un sistema o producto tal que refleja exactamente los requisitos especificados para ese sistema o producto.
Fiabilidad	Propiedad de comportamiento y resultados consistentes.
Gestión del Riesgo	Proceso de evaluar y cuantificar el riesgo y establecer un nivel aceptable de riesgo para la organización.
Gobernanza corporativa	El sistema por el cual se dirigen y controlan las organizaciones. (Adaptado de Cadbury 1992, y OCDE 1999)
Gobernanza corporativa de la TI	El sistema por el cual se dirige y controla el uso, actual y futuro, de la TI. La Gobernanza corporativa de la TI implica evaluar y dirigir la utilización de la TI para dar soporte a la organización y la monitorización de ese uso para lograr la consecución de los planes. Incluye la estrategia y políticas para la utilización de la TI en la organización.
Grupo	Colección de departamentos, directores e individuos que tienen la responsabilidad de un conjunto de tareas o actividades. El tamaño puede variar desde un individuo único a tiempo parcial, hasta varios individuos asignados a tiempo parcial de diferentes departamentos, hasta varios individuos dedicados a tiempo completo.
Grupo de Ingeniería	Conjunto de individuos (tanto directores como personal técnico) que son responsables de las actividades del proyecto o de la organización relacionadas con una disciplina particular de ingeniería (por ejemplo, hardware, software, gestión de configuración software, aseguramiento de la calidad software, sistemas, pruebas del sistema, seguridad del sistema).
Integridad de Datos	Propiedad de que los datos no han sido alterados o destruidos de forma no autorizada.

Término	Definición
ITGI	Information Technology Governance Institute
Línea Base	Especificación o producto que ha sido formalmente revisado y acordado, que sirve como la base para el desarrollo posterior, y que sólo puede cambiarse mediante procedimientos formales de control de cambios.
Margen de ganancia	Es la diferencia entre el precio de venta, sin IVA y los costos de producción o de adquisición de un producto. Es posible calcular distintos márgenes dependiendo de los costos que se imputan al producto: el margen bruto es la diferencia entre el precio de venta (sin IVA) de un bien o servicio y el precio de compra de ese mismo producto, suele ser unitario y se expresa en unidades monetarias/unidad vendida. El margen neto es el margen de beneficio después de los impuestos; esto es, el margen bruto unitario menos los impuestos repercutibles en ese producto. También se expresa en unidades monetarias/unidad vendida.
Organización	Cualquier entidad corporativa, incluyendo asociaciones, clubs, socios, agencias gubernamentales, empresas públicas y privadas.
Política de Seguridad	Conjunto de procesos que gestionan, protegen y distribuyen reglas, directivas y prácticas que gobiernan los activos, incluyendo información sensible, dentro de una organización y sus sistemas.
Procedimiento	Descripción escrita del curso de una acción a llevar a cabo para realizar una tarea dada.
Proceso	Secuencia de pasos realizados para un propósito dado.
Producto de Trabajo	Resultado de un proceso.
Requisitos Relativos a la Seguridad	Requisitos que tienen un efecto directo sobre la operación segura de un sistema para una política especificada de seguridad.
Riesgo	Potencial que una amenaza dada aprovechará las vulnerabilidades de un activo o grupo de activos para causar pérdida o daño a los activos.
Riesgo residual	Riesgo que permanece después de que se han implementado las salvaguardas.
ROA	Return on assets (rendimiento sobre los activos) relaciona la utilidad neta obtenida en un período con el total de activos. Por cada unidad monetaria invertida en activos, la empresa obtiene X de utilidad neta.

Término	Definición
ROE	Return on equity (rentabilidad financiera) relaciona el beneficio económico con los recursos necesarios para obtener ese lucro. La rentabilidad puede verse como una medida de cómo una compañía invierte fondos para generar ingresos. Se suele expresar como porcentaje $ROE = \frac{Beneficio\ Neto}{Patrimonio\ Neto}$.
ROI	Return on investment (retorno de la inversión) sirve para medir la viabilidad de un proyecto. Se utiliza junto al VAN y a la TIR. Existen diversas formas para obtenerlo. Una de ellas es: $ROI = \frac{B}{C_i} \cdot 100$, donde B = beneficios y Ci = costos iniciales. El VAN - Net present value (Valor actual neto) es un procedimiento que permite calcular el valor presente de un determinado número de flujos de caja futuros, originados por una inversión. La metodología consiste en descontar al momento actual (es decir, actualizar mediante una tasa) todos los flujos de caja futuros del proyecto. A este valor se le resta la inversión inicial, de tal modo que el valor obtenido es el valor actual neto del proyecto. La fórmula que nos permite calcular el VAN es: $VAN = \sum_{t=1}^n \frac{V_F}{(1+k)^t} - I_0$ donde: VF representa los flujos de caja, Io es el valor del desembolso inicial de la inversión, n es el número de períodos considerados y k el tipo de interés. Cuando el VAN toma un valor igual a 0, pasa a llamarse TIR (tasa interna de retorno) que es la rentabilidad que nos está proporcionando el proyecto.
SCM	Sistema de administración de la cadena de suministro. Asisten a administrar las relaciones con proveedores, empresas de compras, distribuidores y compañías de logística.
Sistema	Colección de componentes organizados para cumplir una función específica o conjunto de funciones. Un sistema puede incluir muchos productos. Un producto puede ser el sistema.
TI	Recursos requeridos para adquirir, procesar, almacenar y diseminar información.
Validación	Proceso de evaluar un sistema para determinar si satisface los requisitos especificados.
Verificación	Proceso de evaluar un sistema para determina si los productos de trabajo de una fase dada de desarrollo satisfacen las condiciones impuestas al principio de esa fase.
Vulnerabilidad	Incluye una debilidad de un activo o grupo de activos que pueden ser aprovechadas por una amenaza.
ERM	Gestión del Riesgo Empresarial (del inglés Enterprise Risk Management), corresponde al desarrollo de una estrategia en la gestión de riesgos a utilizar por las empresas.

Término	Definición
SECI	Proceso de creación de conocimiento a través de la conversión entre conocimiento tácito y explícito (Socialización, Externalización, Combinación, Internalización).
BA	Contexto compartido en el cual el conocimiento es compartido, creado y utilizado. Plataforma donde se da la conversión del conocimiento.
CKO	Gerente del Conocimiento (acrónimo en Inglés de Chief Knowledge Officer), es el principal responsable de la gestión del conocimiento en las organizaciones. Es el encargado de iniciar, impulsar y coordinar los programas de Gestión del Conocimiento.
CIO	Gerente de Información (acrónimo en Inglés de Chief Information Officer), es el cargo ejecutivo del responsable de la tecnología de la información. Responsable y líder de la estrategia y los sistemas informáticos necesarios para apoyar los objetivos y metas de la organización.
CHRO	Gerente de Recursos Humanos (acrónimo de Chief Human Resource Officer) es el cargo ejecutivo del responsable de la gestión de los recursos humanos de una organización. Es responsable de la atracción, selección, formación, evaluación y recompensa de los empleados, mientras que también supervisa el cumplimiento de las leyes laborales y de empleo.
CMS	Sistema de Gestión de Contenidos (del Inglés Content Management System), es el sistema utilizado para crear, editar, gestionar y publicar contenido de una manera organizada y sistemática.
CEO	Director ejecutivo (acrónimo de Chief Executive Officer), es el responsable y máxima autoridad en la gestión y dirección administrativa de la organización.
Socialización	Proceso de conversión de nuevo conocimiento tácito a través de experiencias compartidas.
Externalización	Proceso de articular el conocimiento tácito en conocimiento explícito.
Combinación	Proceso de convertir el conocimiento explícito en series más complejas y sistemáticas de conocimiento explícito.
Internalización	Proceso de incorporar el conocimiento explícito al conocimiento tácito.
Generación	Actividades para incrementar el stock del conocimiento, con lo cual ampliamos la cantidad y calidad de nuestro almacén de conocimiento.

Término	Definición
Codificación	Poner el conocimiento disponible de forma que sea accesible a quienes lo necesitan, de una forma legible, entendible y organizada.
Transferencia	Transmitir el conocimiento por medios formales e informales.
Identificación	Determinar dónde está el conocimiento y que es lo que falta conocer.
Adquisición	Adquisición del faltante de conocimiento.
Desarrollo	Desarrollar nuevas habilidades, productos e ideas, mejorar procesos y hacerlos más eficientes.
Compartir o Distribuir	Intercambiar el conocimiento disponible a quien lo requiera.
Retención del Conocimiento	Almacenamiento y actualización del conocimiento, por medio de procesos de selección, almacenamiento y actualización regular del conocimiento, de forma estructurada y organizada.
Uso	Utilización del conocimiento por quien lo requiera.
Herramienta de Accesibilidad	Implica que el conocimiento está disponible para quien lo necesita.
Diseño del Área de Trabajo	Definir y organizar el lugar de trabajo de forma que favorezca el intercambio de conocimiento.
Memoria Organizacional	Representación de los conocimientos de una organización en forma explícita y persistente.
Mapa de Conocimiento	Forma de representación del conocimiento para que pueda ser consultado por quien lo necesite.
Patente	Registro del conocimiento.
Benchmarking	Determinar dónde estamos y a donde queremos llegar.
Fusión o Adquisición	Asociarse o comprar conocimiento para la organización.
Lecciones Aprendidas	Registro de lo aprendido para su uso posterior.
Grupos de Expertos	Grupo de personas expertas o especialistas en determinadas áreas y que aportan conocimiento a la organización
Comunidades de Práctica	Grupo de personas que comparten un interés, conjunto de problemas o posesión por un tema y que profundizan sus conocimientos.
Redes	Grupos de personas con determinados roles o intereses comunes.

Término	Definición
Mejores Prácticas	Registrar las mejores formas de realizar una tarea para que la pueda consultar quien lo necesite.
Análisis de Redes Sociales	Utilización de las redes sociales como forma de compartir e intercambiar conocimiento.
Cámara Web	Utilización de la imagen como forma de crear, almacenar y compartir conocimiento.
Videoconferencia	Utilización del video, imagen y sonido como forma de generar y compartir conocimiento.
Realidad Virtual	Simulación de una situación de la realidad como forma de generar y compartir conocimiento.
Sistemas Expertos	Utilización de sistemas especializados en determinada área del conocimiento.
Charlas Informales	Compartir experiencia y conocimiento entre distintos miembros en la organización de manera no planificada.
Coaching	Consulta y asesoramiento con una persona que pueda aportar de su conocimiento.
Mentoring	Crecimiento personal de una persona de forma abarcativa y general a través de un mentor, quien aconseja y enseña gradualmente en base a su experiencia.
Bases de Conocimiento	Bases de datos que contienen conocimiento para ser utilizado por quien lo necesite.
E-Learning	Forma electrónica de aprendizaje para lograr adquirir un determinado conocimiento.
Clasificación	Ordenar el conocimiento de forma que sea de más fácil acceso para quien lo requiera.
Clustering	Agrupar el conocimiento en determinados grupos de interés, roles, o algún criterio para que sea de fácil acceso a quien lo necesite y lo deba tener.
Factor Recurso Económico	Provisión de los recursos financieros necesarios para el desarrollo de las actividades de Gestión del Conocimiento.
Factor Tiempo	Dedicación de tiempo para las actividades de Gestión del Conocimiento.
Capacitación	Provisión de entrenamiento relativo a la mejora de la Gestión del Conocimiento.
Recursos Humanos	Provisión de las personas necesarias para el desarrollo de las actividades de Gestión del Conocimiento
Marco de buenas practicas	Existencia de un conjunto de formas de realizar determinada tarea para el logro de una eficiente Gestión del Conocimiento.
Cultura Organizacional	Existencia de una forma de gestionar el conocimiento que sea entendida y aplicada por todos los miembros de la organización.

Término	Definición
Compromiso de la Alta Gerencia	Compromiso y apoyo de los ejecutivos y de la alta gerencia a la Gestión del Conocimiento
Creatividad	Proceso que lleva a una repentina visión para resolver un problema
Ontología	Descripción explícita formal de un concepto en un dominio determinado, propiedades de cada concepto describiendo sus características y atributos, así como relaciones entre estas.
Marcos	Estructura de datos que representa situaciones estereotipadas construidas en base a experiencias similares ocurridas en el pasado, permitiendo luego aplicar los conocimientos de estas situaciones, eventos y conceptos previos a nuevas situaciones.
Redes Semánticas	Técnica de representación de conocimientos donde se expresan conceptos de un dominio y sus relaciones con grafos dirigidos, que permiten una visualización gráfica.
Educción del Conocimiento	Proceso que sigue una serie de etapas (Preparación, Sesión, Transcripción, Análisis y Evaluación) para lograr la explicación del conocimiento tácito de los expertos.
Ingeniero de Conocimiento	Conjunto de principios, métodos y herramientas que permiten aplicar el saber científico y de experiencias a la utilización de los conocimientos y sus fuentes.
Capital Intelectual	Suma de todos los conocimientos de todos los empleados de una empresa que le dan una ventaja competitiva.

Índice

Declaración de autoría.....	2
Agradecimientos.....	3
Abstract	4
Palabras clave	5
Glosario	6
Índice de Figuras	18
Índice de Tablas	19
1. Introducción y objetivo del trabajo.....	20
1.1. Introducción.....	20
1.2. Objetivos.....	20
1.3. Hipótesis.....	21
1.4. Pertinencia	22
2. Estado del Arte	23
2.1. Tecnologías de la Información.....	23
2.2. Gobierno Corporativo.....	24
2.2.1. OCDE	25
2.2.2. Código de Buen Gobierno KING III.....	26
2.3. Gobierno de TI.....	26
2.3.1. ISO/IEC 38500	27
2.3.1. Elementos de la gobernanza de TI.....	28
2.3.2. Diseño de la Gobernanza de TI.....	28
2.3.3. Mejora continua para un buen Gobierno de TI.....	29
2.3.4. Riesgos y Estrategias en el diseño de la Gobernanza de TI.....	30
2.4. Marcos de buen gobierno de TI.....	30
2.4.1. Norma AS 8015 de Gobernanza de TI.....	31
2.4.2. Norma ISO/IEC 38500:	31
2.4.3. Marco de gobernanza de TI: Calder – Moir	33
2.4.4. Marcos de gestión de TI.....	34
2.5. Buen Gobierno de TI	38
2.5.1. Objetivos del buen Gobierno de TI.....	39
2.5.2. Dominios del buen Gobierno de TI	41
2.5.3. Gobierno de TI vs Gestión y Control de TI.....	42
2.6. Gobernanza de TI en PyMEs.....	43

2.6.1.	<i>Alineamiento estratégico de TI en PyMEs del Uruguay</i>	43
2.6.2.	<i>Riesgo desde el punto de vista de la Gestión del Conocimiento</i>	44
2.7.	Definición de Conocimiento.....	45
2.7.1.	<i>Propiedades del Conocimiento</i>	45
2.7.2.	<i>Gestión del Conocimiento</i>	46
2.7.3.	<i>Historia de la gestión del conocimiento</i>	47
2.7.4.	<i>Procesos de gestión del conocimiento</i>	49
2.7.5.	<i>Herramientas, Técnicas y Factores</i>	50
2.7.6.	<i>Creatividad y Conocimiento</i>	51
2.7.7.	<i>Mapas de Conocimiento</i>	51
2.7.8.	<i>Ontologías</i>	52
2.7.9.	<i>Marcos</i>	53
2.7.10.	<i>Redes Semánticas</i>	53
2.7.11.	<i>Edución del Conocimiento</i>	54
2.7.12.	<i>Representación informática del conocimiento</i>	54
2.7.13.	<i>Capital Intelectual e Ingeniería del Conocimiento</i>	55
2.8.	Chief Knowledge Officer (CKO)	55
2.8.1.	<i>Estrategia de Gestión del Conocimiento</i>	55
2.8.2.	<i>Relación entre Gestión del Conocimiento y Gobierno de TI</i>	56
2.8.3.	<i>Análisis de las etapas a utilizar</i>	56
3.	Marco de Gestión de Riesgos de TI en Función de la Gestión de Conocimiento	59
3.1.	Introducción.....	59
3.2.	Marco de Gestión del Conocimiento Aplicado al Riesgo en TI	59
3.3.	Modelo de Madurez de Gestión del Conocimiento Aplicado al Riesgo en TI	61
4.	Indicadores	63
4.1.	Ponderación de indicadores según el nivel de madurez	63
5.	Experimentación	64
5.1.	Planificación.....	64
5.2.	Ejecución	78
5.3.	Conclusión y Evaluación.....	96
6.	Conclusiones y trabajo futuro	100
7.	Referencias	103
ANEXOS	111
ANEXO I - Estudio empírico sobre los problemas de gobernabilidad de TI en empresas de tipo PyMEs y recomendaciones para mitigarlos		112

ANEXO II - Knowledge Management Steps, Tools, Techniques and Influencing Factors in SMEs ..	133
ANEXO III - Modelo de Madurez de Alineamiento Estratégico de TI en empresas de tipo PyMEs y resultados de la aplicación de este modelo en estas organizaciones.....	158
ANEXO IV - Encuesta sobre Alineamiento Estratégico de TI en las PyMEs de Uruguay	184
ANEXO V - Características y estado de la Gestión del Conocimiento en las PYMES del Uruguay..	238
ANEXO VI - Estudio de la incidencia de la cantidad de empleados – cantidad de empleados de TI.	264
Anexo VII - Guía de relevamiento	324
Anexo VIII – Experiencia en Risk IT.....	356
Anexo IX – Ikujiro Nonaka e Hirotaka Takeuchi.....	361
Anexo X – Estrategia de Gestión del Conocimiento.....	370
Anexo XI – Chief Knowledge Officer.....	372
Anexo XII – Relación entre Gestión del Conocimiento y Gobierno de TI	375
ANEXO XIII – Riesgo desde el punto de vista de la Gestión del Conocimiento	381
Anexo XIV – Matrices del Marco de Gestión del Riesgo basado en la Gestión del Conocimiento....	384
Anexo XV – Matrices del Modelo de Gestión del Riesgo basado en la Gestión del Conocimiento...	461
Anexo XVI – Indicadores para el Modelo de Gestión del Riesgo basado en la Gestión del Conocimiento	480
Anexo XVII – Justificación y ponderación de indicadores	512

Índice de Figuras

Figura 1 ELEMENTOS CLAVE DEL SISTEMA DE NEGOCIO. TOMADO DE [29]	28
Figura 2 Marco para diseñar el Gobierno de TI. Tomado de [28]	29
Figura 3 MODELO DE CONTROL ADAPTADO DE [4]	29
Figura 4 CICLO DE MEJORA CONTÍNUA (PDAC). TOMADO DE [31]	30
Figura 5 MODELO DE BUEN GOBIERNO CORPORATIVO DE TI. TOMADO DE [35].....	32
Figura 6 OBJETIVO DE LA GOBERNANZA. TOMADO DE [5]	35
Figura 7 RELACIONES CAUSA EFECTO. ADAPTADO DE [43]	37
Figura 8 CASCADA DE CUADROS DE MANDO. ADAPTADO DE [43].....	37
Figura 9 Información de interés del mundo TI [online] [15 junio 2010]. Disponible en Internet :< http://www.helkyncoello.wordpress.com >.....	38
Figura 10 El gobierno TI garantiza la alineación de la función TI con las necesidades de su negocio. Gobierno de TI [online] [17 junio 2010]. Disponible en Internet :< http://www.agaex.com >.....	40
Figura 11 Información de interés del mundo TI [online] [15 junio 2010]. Disponible en Internet :< http://www.helkyncoello.wordpress.com >	41
Figura 12 Información de interés del mundo TI [online] [15 junio 2010]. Disponible en Internet :< http://www.helkyncoello.wordpress.com >.....	41
Figura 13 Información de interés del mundo TI [online] [15 junio 2010].	42
Figura 14 A knowledge source map for a multimedia company (excerpt).....	52
Figura 15 Planilla de Experimentación	65
Figura 16 Planilla resultado de las encuestas	79
Figura 17 Porcentaje de indicadores en cada dominio según su nivel en el modelo	96
Figura 18 Indicadores por categoría y nivel para la empresa informática.....	98
Figura 19 Indicadores por categoría y nivel para la empresa inmobiliaria.....	98
Figura 20 Porcentaje de mejora en el modelo y costo asociado por categoría de los indicadores	99

Índice de Tablas

Tabla 1 Vínculo entre procesos/actividades Risk IT y Gestión del Conocimiento.....	59
Tabla 2 Vínculo entre procesos/actividades de Risk IT y etapas, herramientas, técnicas y factores de Gestión del Conocimiento	60
Tabla 3 Matriz RACI de procesos/actividades de Risk IT de un dominio para cada rol	61

1. Introducción y objetivo del trabajo

1.1. Introducción

Este trabajo presenta un marco de buenas prácticas y modelo de madurez para la gestión de riesgos en empresas de tipo PyMEs en la República Oriental del Uruguay desde la perspectiva de la Gestión del Conocimiento. La aplicación del marco de buenas prácticas permitirá la mejora en la Gestión de riesgos y la implementación del modelo de madurez posibilitara determinar en qué nivel se encuentra la organización así como los procesos y actividades del siguiente nivel necesarios para el logro de la mejora en la gestión del riesgo.

Para ello se analizan las relaciones entre Gobierno de TI, fundamentalmente en el área de Gestión de Riesgos, en función de la Gestión del conocimiento.

En primera instancia se realiza un estudio del estado del arte de Gobierno de TI y Gestión del conocimiento, analizando las relaciones entre ambos y estudiando la incidencia de la gestión del conocimiento en la gestión del riesgo específicamente.

A continuación se revisa el modelo de madurez en Gobernanza de TI para PyMEs presentado en [1] para las empresas de tipo PyMEs en la República Oriental del Uruguay.

Luego se realiza una revisión sistemática de gestión del conocimiento en empresas de tipo PyMEs y se realiza un estudio empírico de gestión del conocimiento y gestión de riesgos en PyMEs de Uruguay [2], a través de los cuales se establece la necesidad de un marco de gestión de riesgos basado en la gestión del conocimiento.

Posteriormente se define un marco de buenas prácticas y modelo de madurez de gestión de riesgos basado en la gestión del conocimiento para empresas de tipo PyMEs en la República Oriental del Uruguay.

Seguidamente se realiza una validación del modelo planteado, a través de 3 expertos en gestión del riesgo para contar con elementos de mejora en su elaboración y lograr así un modelo más robusto en cuanto a la gestión de riesgos.

Habiendo validado el marco, se implementa el mismo en PyMEs de Uruguay como casos de estudio, analizándose y publicándose los resultados de esta implementación.

Finalmente se desarrollan las conclusiones del trabajo realizado y se plantean trabajos futuros.

1.2. Objetivos

El objetivo de esta tesis es desarrollar e implementar un marco de buenas prácticas y modelo de madurez para la gestión de riesgos en empresas de tipo PyMEs en la República Oriental del Uruguay desde la perspectiva de la Gestión del Conocimiento.

De esta forma los objetivos específicos del trabajo son los siguientes:

- Desarrollo de un marco de buenas prácticas en la gestión del conocimiento para la gestión del riesgo.

- Desarrollo de un modelo de madurez de gestión de riesgos basado en la gestión del conocimiento.
- Validación del modelo planteado en empresas PyMEs de Uruguay
- Análisis y publicación de resultados obtenidos

1.3. Hipótesis

1. Existe una relación entre la gestión del conocimiento y la gestión del riesgo.

Justificación: Según [2] las organizaciones necesitan tomar decisiones rápidas y adecuadas para lograr nuevas oportunidades, ventajas competitivas sostenibles y la continuidad del negocio. Esto es posible si se cuenta con el conocimiento necesario de forma oportuna, adecuada y en el lugar apropiado, para lo cual se debe gestionar el conocimiento de una manera eficiente. Según [1] la gestión del riesgo es un elemento fundamental en la buena gobernanza de TI, podemos ver de esta manera la importancia que tiene la gestión del conocimiento aplicada en la gestión del riesgo en TI.

2. A una mayor eficiencia en la gestión del conocimiento se obtiene una mayor eficiencia en la gestión del riesgo.

Justificación: Según [1] se puede ver que la relación encontrada en la hipótesis 1 también indica que a mejor gestión del conocimiento, se tendrá mayor eficiencia en la gestión del riesgo. Un caso de éxito de la buena gestión del riesgo en función de la buena gestión del conocimiento se da en la organización Chrysler [3] donde se muestra un caso de éxito en la implementación de una fábrica de experiencia y la incidencia de la gestión del conocimiento en la gestión del riesgo. En un período de tres años, un grupo de apoyo en gestión de calidad impulsó un proceso de software de manejo de riesgos, desarrollando proyectos piloto, discutiendo el proceso en grupos de usuarios, remitiéndolo a la administración por aprobación, ofreciendo entrenamiento en cursos adaptados, y usando una base de experiencias en el manejo de riesgos específica y personalizada. El grupo consideraba a todos los accionistas y sus preocupaciones, diferencias y requerimientos, anticipando y atendiendo la necesidad de entrenamiento.

Esto permitió que el manejo del riesgo sea ahora aceptado en todo el departamento y aplicado en todos los altos procesos de software estratégicos así como a un creciente número de otros proyectos de software. Los riesgos son ahora identificados tempranamente y pueden ser mitigados de forma más efectiva.

3. No existe un marco de buenas prácticas y un modelo de madurez aplicado a PyMEs.

Justificación: Se encontró en el estado del arte de gestión del conocimiento y de gobierno de TI específicamente en gestión de riesgos, así como en la revisión sistemática de la literatura realizada, que no hay evidencia de la existencia de un marco de gestión del riesgo aplicado a PyMEs, así como la existencia de un marco que establezca directamente como incide la gestión del conocimiento, sus procesos y prácticas, en la gestión del riesgo.

1.4. Pertinencia

La adecuada gestión del riesgo es fundamental para una buena Gobernanza de TI [4]. Favorece el logro de los objetivos organizacionales y permite la continuidad del negocio.

Existen en la industria varios marcos y estándares de buenas prácticas para Gobierno de TI como COBIT [4], actualmente COBIT 5 [5], Val IT [6], ITIL [7], ISO 38500 [8], Calder Moir [9] y MOF [10] que si bien consideran al riesgo como una de las áreas de enfoque de Gobierno de TI, no son específicos ni se especializan en la gestión del riesgo. Aún en el marco Risk IT [11] que si bien se vincula con COBIT [4] y Val IT [6], es más específico en la gestión de riesgos, tampoco existe una incorporación formal de buenas prácticas de gestión del conocimiento a la gestión de riesgos y muchas de las buenas prácticas que se presentan para gestionar el riesgo no aplican a las Pymes en Uruguay [2].

La gestión del riesgo tiene un estrecho vínculo con la gestión del conocimiento. Si la organización gestiona adecuadamente el conocimiento e incorpora, preserva, disemina y utiliza el conocimiento de manera inteligente, tendrá la información necesaria para poder gestionar adecuadamente el riesgo, previniendo, mitigando o eliminando el mismo en la organización.

En el Uruguay, se considera como pequeña empresa a las de hasta 19 trabajadores y mediana empresa a las que poseen entre 20 y 99. Esta clasificación varía según el país que se considere, siendo en general mayores los límites de cada intervalo a mayor tamaño del país y volumen económico.

La realidad del mercado industrial en el Uruguay hace que las empresas categorizadas como PyMEs [12] tengan una incidencia fundamental; según la DINAPYME (Dirección Nacional de Artesanías, Pequeñas y Medianas Empresas. Ministerio de Industria, Energía y Minería – República Oriental del Uruguay) [13] el 99% de las unidades económicas productivas del sector privado del Uruguay son PyMEs y el 70% de las personas trabaja en empresas tipificadas como tales [14]. Esta particularidad hace que sea altamente relevante analizar elementos de gobierno de TI aplicados a este tipo de empresas. Éste tipo de empresa aporta el 33% de PBI y el 25% de la inversión [15].

También las PyMEs son muy importantes en las distintas economías del mundo. Estadísticas de la SBA [16] de Estados Unidos muestran que en el 2007 las pequeñas empresas generaron alrededor del 50% de todas las ventas estadounidenses, y también contribuyeron al 50 % del PBI privado. Además, emplearon a más del 50% de la fuerza laboral de ese país [17].

Es por las razones anteriormente mencionadas en la hipótesis 2 [3], que atendiendo a la necesidad de una adecuada gestión de riesgos en las PyMEs donde se considere a la gestión del conocimiento como elemento fundamental para el logro de este objetivo se plantea como desafío la creación de un marco de buenas prácticas para la gestión del riesgo en Pymes basada en la gestión del conocimiento para conseguir prevenir, mitigar o eliminar el riesgo en las mismas.

2. Estado del Arte

2.1. Tecnologías de la Información

La información y la tecnología que recoge, almacena y distribuye la información se encuentra entre los recursos y activos más importantes para la diferenciación y el logro de ventajas competitivas de una organización siendo de suma importancia el alineamiento de las tecnologías de la información con las metas y objetivos organizacionales.

Dentro de los distintos recursos que se manejan en las organizaciones como personal, dinero, establecimiento, y servicio de atención al cliente entre otros; la tecnología que recoge, almacena y distribuye la información, está entre los activos que se encuentran más difíciles de comprender y administrar. [18]

Las implementaciones en TI, involucran inversiones tanto por adelantado como una vez en curso, y las ganancias no son predecibles ya que los negocios requieren cambios constantes. Estas incertidumbres y complejidades llevan a muchos directores de empresas a abdicar en su responsabilidad de hacer que su gente utilice la TI efectivamente.

Durante muchos años, algunas organizaciones han podido tener éxito a pesar de sus débiles prácticas en el manejo de TI. Pero la información, y por ende la TI es un elemento cada vez más importante de la organización, los productos, los servicios y el fundamento de los procesos empresariales. El estrecho vínculo entre TI y los procesos organizativos implica que la unidad de TI por sí sola, no puede hacerse cargo de la responsabilidad que implica el uso efectivo de la información o la tecnología de la información. El obtener mayores beneficios de la TI es cada vez más una responsabilidad organizacional. Corresponde a los líderes de las empresas, el desarrollar esa capacidad.

La Tecnología de la información permite aumentar la competitividad de la organización teniendo como objetivo las prioridades estratégicas de la empresa no así las tácticas. Entendemos la estrategia como una serie de elecciones como el determinar quiénes son los clientes a los que se apunta, cuáles son los productos y servicios que se ofrecen y cuál es la posición única y valiosa a la que apunta la firma y qué procesos centrales incorporan la posición única de la firma en el mercado. [18]

Es muy importante que los directores de la empresa reconozcan la responsabilidad que tienen en la toma de decisiones y el uso y manejo efectivo de TI y no asuman que la responsabilidad es del departamento de TI.

Las empresas destacadas tienen éxito mientras que otras fracasan en implementar un Gobierno de TI efectivo que apoye sus estrategias. Por ejemplo: las firmas con un Gobierno de TI superior al promedio que siguen una estrategia específica (p. ej.: seguimiento del cliente), obtienen un 20% más de beneficios que las firmas que siguen la misma estrategia, pero que tienen un Gobierno de TI pobre.

Las empresas más destacadas manejan TI en forma diferente que otras empresas. Conscientes de las fuerzas competitivas internas, las empresas destacadas diseñaron estructuras de manejo vinculadas a la medida de rendimiento en la que sobresalían (Por ejemplo: crecimiento o ganancia de activos), armonizando de esa forma los objetivos empresariales, la estrategia de

gobierno, sus mecanismos y los objetivos de rendimiento y su métrica. En resumen: El diseño de un buen gobierno le permite a las empresas obtener resultados superiores en sus inversiones en TI.

Se concluye que un manejo efectivo de TI, es por sí solo el elemento más importante a fin de predecir el valor que una organización generará de TI.

2.2. Gobierno Corporativo

Diversos autores [19-26], definen a la “Gobernanza Corporativa” como el sistema por el cual las empresas son dirigidas y administradas estableciendo la estructura a través de la cual se establecen los objetivos de la empresa así como los medios para alcanzarlos y realizar el seguimiento de su desempeño. Se establece que el rol de los accionistas es nombrar a los responsables de ejecutar y auditar los procesos de gobernanza.

Para poder abordar con profundidad el Gobierno de TI debemos analizar el tema del gobierno en las empresas. El gobierno corporativo, se ha convertido en un tema dominante en los negocios.

Existen diversas directrices para un buen gobierno corporativo. El gobierno corporativo debe proveer la estructura para determinar los objetivos organizativos y monitorear el desempeño a fin de asegurar el logro de los objetivos.

Debe existir un marco de trabajo común en el cual la corporación debe estar unida y alineada con el Gobierno de TI.

Las conductas deseables, representan las creencias y la cultura de la organización tal como se define y lleva a cabo mediante no solo la estrategia, sino las declaraciones de valores corporativos, declaraciones de cometido, principios empresariales, rituales y estructuras. Las conductas deseables varían de una empresa a otra. Son las conductas, no las estrategias, las que generan valores.

Identificamos seis activos clave mediante los cuales las empresas alcanzan sus objetivos y logran valor empresarial. Los equipos directivos crean mecanismos para gobernar el control y uso de cada uno de estos activos independientemente y en conjunto. Los elementos clave de cada activo, incluyen lo siguiente.

- **Activos humanos**

Personas, habilidades, trayectoria profesional, entrenamiento, presentación de informes, aptitud, tutoría, etc.

- **Activos financieros**

Dinero, inversiones, obligaciones financieras, flujo de dinero, entradas, etc.

- **Activos físicos**

Edificios, fábricas, equipamiento, mantenimiento, seguridad, utilización, etc.

- **Activos de propiedad intelectual**

Propiedad intelectual que incluye: productos, servicios y procesos de saber cómo formalmente patentados, registrados o incluidos en las personas o los sistemas de la empresa.

- **Activos de información**

Información digitalizada, información y conocimiento sobre los clientes, desempeño de los procesos, finanzas, sistemas de información, etc.

- **Activos de relacionamiento**

Relacionamiento dentro de la empresa así como el relacionamiento con la marca, y la reputación entre los clientes, proveedores, unidades empresariales, reguladores, competidores, canal de socios, etc.

El manejo de los activos principales, se da a través de un gran número de mecanismos organizativos (por ejemplo: estructuras, procesos, comités, procedimientos y auditorías). Algunos mecanismos son únicos para determinado activo (por ejemplo: el comité de arquitectura de TI), mientras otros cruzan e integran múltiples tipos de activos (el proceso de aprobación del presupuesto, por ejemplo), asegurando la sinergia entre los activos clave. La madurez en el manejo de los seis activos clave, varía significativamente en la mayoría de las empresas, siendo en general los activos financieros y físicos los mejor manejados y los activos de información los peor manejados.

En general las empresas con mecanismos comunes para varios activos, se desempeñan mejor. Por ejemplo: si el mismo comité ejecutivo se encarga de controlar tanto los activos financieros como los de TI, una firma puede alcanzar mayor integración, creando mayor valor. Algunos mecanismos, seguirán siendo únicos para cada activo, (el comité auditor para el activo financiero y el comité de TI, para TI por ejemplo), pero algunos mecanismos comunes, llevan a una mejor coordinación de los seis activos.

La evaluación promedio de un grupo de 42 CIOs sobre cuán bien integraban el manejo de TI con el manejo de los otros activos clave, arrojó que menos de un 5% tenían una buena integración de TI con otros activos [18] El crear mecanismos comunes de manejo entre los activos, no solo incrementará la integración, sino que además, el número menor de mecanismos resultantes será más fácil de comunicar e implementar. La educación del comité ejecutivo sobre cómo los mecanismos de gobierno se combinan para trabajar en bien de la empresa, es una tarea constante y necesaria para un gobierno efectivo. Afirmamos que muchos beneficios tangibles se desprenderán de un mejor manejo de TI.

2.2.1. *OCDE*

La OCDE es la Organización para la Cooperación y el Desarrollo Económicos que tiene como objetivos lograr el mayor crecimiento sostenible posible de la economía y del empleo y aumentar el nivel de vida en los países miembros, manteniendo la estabilidad financiera y contribuyendo así al desarrollo de la economía mundial, contribuir a una sana expansión económica tanto en los Estados miembros como en los no-miembros en vías de desarrollo económico y a contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria, de acuerdo con las obligaciones internacionales.

Los Principios del Buen Gobierno Corporativo de la OCDE son:

1. Garantizar la Base de un Marco Eficaz para el Gobierno Corporativo
2. Los Derechos de los Accionistas y Funciones Clave en el Ámbito de la Propiedad
3. Tratamiento Equitativo de los Accionistas

4. El Papel de las Partes Interesadas en el Gobierno Corporativo
5. Revelación de Datos y Transparencia
6. Las Responsabilidades del Consejo

2.2.2. *CÓDIGO DE BUEN GOBIERNO KING III*

El Código de buen gobierno KING III, hito importante en la evolución de la gobernabilidad de las empresas en Sudáfrica, gira en torno a los siguientes principios: liderazgo, sostenibilidad y ciudadanía corporativa.

Los principios del Código de Gobierno Corporativo KING III son:

- El buen gobierno es eficaz en el liderazgo
- La sostenibilidad es un principio moral, un imperativo económico y es una importante fuente de oportunidades
- La innovación, la equidad y la colaboración son aspectos clave de cualquier transición hacia la sostenibilidad
- La transformación social y la reparación es importante y tiene que integrarse dentro de lo más amplio de transición hacia la sostenibilidad
- La consideración del papel estratégico de las TI y su importancia desde la perspectiva de la gobernanza

A su vez reconoce que las TI se han convertido en parte integral del negocio, siendo fundamentales para el apoyo, viabilidad y crecimiento de las organizaciones.

Es así que los principios de gobernanza corporativa de TI KING III son:

- La junta debe ser responsable de la gobernanza de las TI.
- TI debe estar alineada con los objetivos de rendimiento y de sostenibilidad de la empresa.
- La junta directiva debe delegar en la gestión la responsabilidad de la implantación de un marco de gobierno de TI.
- El consejo debe supervisar y evaluar gastos e inversiones significativos en TI.
- La gestión de riesgos de TI debe formar parte integral de la gestión de riesgos corporativa.
- El Consejo debe asegurar que los activos de información son administrados eficazmente.
- Comités de riesgo y auditoría deben asistir a la junta en el cumplimiento de sus responsabilidades de TI

2.3. **Gobierno de TI**

Podemos definir al Gobierno de TI como el definir los derechos de decisión y el marco de rendición de cuentas para alentar una conducta deseable en el uso de TI [18].

Estas conductas son diferentes para cada empresa. El Gobierno de TI no trata sobre tomar decisiones específicas en TI, es la dirección quien realiza esta tarea, sino que el Gobierno de

TI más bien determina quienes toman y contribuyen a esas decisiones. El Gobierno de TI refleja principios de manejo corporativo más amplios mientras se enfoca en el manejo y uso de TI para lograr las metas de desempeño corporativo.

Gobierno de TI es: Alinear las estrategias de TI de una organización con su estrategia general para que esta alcance su meta y objetivo. El Gobierno de TI hereda características del gobierno corporativo y la administración de TI a fin de asegurar la transparencia en el manejo y el control de los activos de TI mediante el gobierno corporativo y el manejo efectivo de los recursos de TI a través de la administración de TI.[18]

Gobierno de TI es *“Es el proceso de administración que asegura la obtención de los beneficios esperados de la tecnología de información (TI) de manera controlada para acrecentar el éxito sostenido de una empresa a largo plazo”* [4]

Gobierno de TI es *“Es el uso eficiente de los recursos de TI para apoyar el cumplimiento de los objetivos del negocio”* [5]

Gobierno de TI es un *“Sistema por el cual el uso presente y futuro de las TI es controlado. Involucra evaluar y dirigir planes del uso de las TI que soporten a la organización, así como monitorear el uso de estos planes. Incluye además políticas y estrategias de uso de TI en la organización.”* [27]

Según Weill y Ross [28], para obtener más valor de las inversiones de TI se debe aclarar las estrategias de negocio y el rol de TI para alcanzarlas, medir y gestionar lo invertido y lo obtenido en TI, asignar valor contable a los cambios surgidos de la aplicación de TI y por último aprender de cada implementación haciendo cada vez más reuso de los recursos y capacidades de TI.

Tomme [29] afirma que el reto al que se enfrentan las organizaciones es alcanzar el éxito con TI, al hacerlo, habilitarán la obtención de beneficios sustanciales.

2.3.1. ISO/IEC 38500

En el año 2008 se publica la norma ISO/IEC 38500 [8] sobre gobernanza de TI donde presenta la definición formal: *“la gobernanza corporativa de TI es el sistema por el cual el uso actual y futuro de TI es dirigido y controlado. La gobernanza de TI implica evaluar y dirigir el uso de las TI para dar soporte a la organización y monitorizar el uso para lograr los planes. Incluye la estrategia y políticas para la utilización de las TI en la organización”*

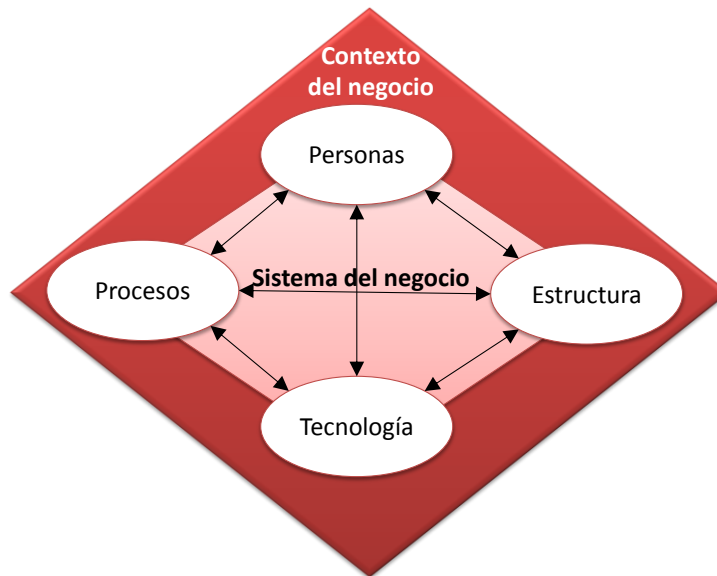


Figura 1 ELEMENTOS CLAVE DEL SISTEMA DE NEGOCIO. TOMADO DE [29]

2.3.1. *ELEMENTOS DE LA GOBERNANZA DE TI*

Para comprender el concepto de gobernanza de TI, se cita a Mark Toomey, el cual hace un estudio comprensivo de la norma ISO/IEC 38500 [8, 29] y a los autores de "*IT Governance. How top performers manage IT decision rights for superior results*" Peter Weill y Jeanne Ross [28].

2.3.2. *DISEÑO DE LA GOBERNANZA DE TI*

Según Weill y Ross en [28] [30], las empresas que poseen un gobierno de TI efectivo armonizan 6 elementos del gobierno expresados en lo que definen como un marco (framework) de gobernanza de TI. En la Figura 2, se muestran dichos elementos (estrategia del negocio y organización, acuerdos de gobierno de TI, objetivos de desempeño del negocio, organización de TI y comportamientos, mecanismos de gobernanza de TI, métricas de TI y contabilidad) y las relaciones entre los mismos. El buen gobierno de TI es una responsabilidad del cuerpo directivo, si no está generando valor entonces el cuerpo directivo deberá como primera acción examinar sus prácticas de gobernanza de TI.

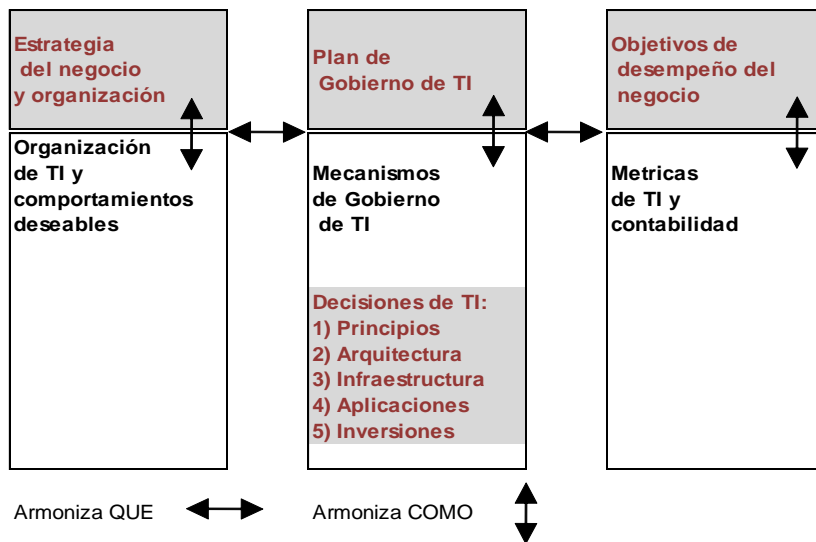


Figura 2 Marco para diseñar el Gobierno de TI. Tomado de [28]

2.3.3. MEJORA CONTINUA PARA UN BUEN GOBIERNO DE TI

El modelo de toma de decisiones y los responsables de las mismas deben estar enmarcados en un modelo de mejora continua que permita el aprendizaje por parte del negocio y de TI permitiendo alcanzar los niveles de calidad de servicio y el valor esperados [4].

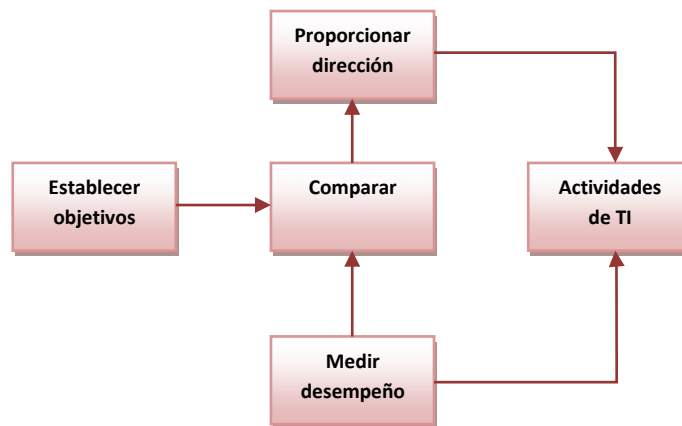


Figura 3 MODELO DE CONTROL ADAPTADO DE [4]

A partir de los principios de TI definidos a nivel estratégico, se establecen objetivos de TI del negocio, proporcionando la dirección inicial. A partir de ahí se establece un circuito continuo de desempeño que se mide y compara con los objetivos, lo que da como resultado una nueva dirección en las actividades cuando sea necesario [4] (Figura 3). Los objetivos o políticas de TI para un buen gobierno de TI no se establecen una única vez, son elementos dinámicos que deben alinearse, modificarse y mejorar conforme cambia el escenario de la organización y de acuerdo a los cambios estratégicos que ésta realice. Es un esquema de retroalimentación y monitoreo continuo, indispensable para que, con el tiempo, la estrategia de TI no quede obsoleta dentro de la organización.

Para establecer un modelo formal de mejora se utiliza una estrategia de mejora continua, el ciclo de Deming [31-33], definida en cuatro pasos PDCA (planificar, hacer, verificar, actuar - en inglés plan, do, check, act). A través de éste modelo se puede lograr la implantación de un ciclo de mejora de procesos (Figura 4), las fases son:

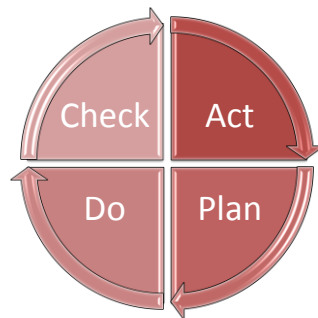


Figura 4 CICLO DE MEJORA CONTÍNUA (PDAC). TOMADO DE [31]

2.3.4. *RIESGOS Y ESTRATEGIAS EN EL DISEÑO DE LA GOBERNANZA DE TI*

Alinear y unir las decisiones de negocio con las de TI en un proceso único de toma de decisión implica riesgos para la organización ya que:

- a) Las decisiones de TI son ejecutadas por los líderes empresariales y de las unidades de TI. Este mecanismo asegura que se cumplan los objetivos del negocio y de las unidades del mismo, pero las decisiones de TI también están dirigidas por los objetivos del negocio, como ser las economías de escala.
- b) Gerentes de división y de línea de producción aprueban sus respectivas estrategias de TI. Estas estrategias contribuyen a la definición de los principios y de las decisiones de inversión del negocio.
- c) Los objetivos de desempeño necesitan que se reduzcan costos y la integración de negocios motiva la adopción de infraestructuras compartidas y estándares de arquitectura.
- d) Las unidades de negocio tienen responsabilidades individuales respecto de las necesidades de aplicaciones, y deben ajustarse a los principios del negocio respecto de comprar-tener-vender.

2.4. **Marcos de buen gobierno de TI**

La información es un elemento presente en todos los aspectos que conforman la actividad del negocio, lo que sustenta la idea de implementar marcos de gobernanza de TI. El ITGI define la gobernanza de TI como: *“la capacidad de liderazgo y las estructuras y procesos organizativos que aseguran que las TI de la organización se extiendan y sustenten a las estrategias y objetivos de la misma”* [34]. Como no todas las empresas poseen la misma estructura, cuando se implementan dichos marcos, aquellos procesos que no son relevantes al contexto de aplicación se evitan ganando eficiencia lo que evidencia cierta dificultad para crear un marco de buen gobierno de TI genérico aplicable a todas las empresas. A medida que los procesos se hacen más complejos y los marcos más completos también se tornan más generales por lo que cada empresa deberá adaptarlos adecuadamente. A continuación se analizan los marcos más difundidos por la literatura.

Se presentan y comparan los estándares y marcos de buenas prácticas relativas al gobierno corporativo y a la gobernanza de las tecnologías de la información. Para poder realizar dicha comparación se utilizará el Método de Estudio de Similitud entre Modelos y Estándares [35].

2.4.1. *NORMA AS 8015 DE GOBERNANZA DE TI*

La Norma Australiana AS 8015 se publica el 31 de enero de 2005, la misma establece que los directores deben regir las Tecnologías de la Información y las Comunicaciones (TICs) a través de tres tareas principales [29]:

- Evaluar el uso de las TICs
- La preparación y puesta en práctica de políticas y planes
- Monitorear la conformidad con las políticas y el desempeño contra los planes.

Estas tres tareas establecen como obligación del director el entender y gestionar los riesgos correctamente, desde el punto de vista de los mismos, la gestión del riesgo es un deber y la misma está estrechamente alineada con la determinación de la estrategia correcta para el negocio. Unos de los objetivos que la norma AS8015 tuvo en su definición fue el de proporcionar a las organizaciones una nueva orientación sobre la manera de garantizar el uso de TI de forma eficaz, eficiente y aceptable. La visión acerca de la gobernanza de TI es que la misma debe habilitar tanto la creación de capacidad a futuro (proyectos) como el día a día (operaciones).

Se establece un nuevo modelo de gobernanza, donde las necesidades y las oportunidades se evalúan, se dirigen, se entregan los proyectos, se llevan a cabo las operaciones comerciales y se controla el rendimiento y la conformidad con las leyes y las regulaciones de todo el sistema de IT.

Esta norma ha sido la semilla a partir de la cual se define la ISO/IEC 38500 [8], que ha sido adoptada como norma a nivel internacional.

2.4.2. *NORMA ISO/IEC 38500:*

Esta norma tiene sus orígenes en el 2005 y fue preparada por el Standars Australia como AS8015:2005, posteriormente la adopta la ISO/IEC dando lugar a la norma ISO/IEC 38500:2008, que fue adaptada recientemente a su versión ISO/IEC 38500:2015[8]. Su objetivo es proveer un marco de principios y buenas prácticas a la hora de evaluar, dirigir y controlar la utilización de TI en las organizaciones. Está alineada con los principios de gobierno corporativo enunciados en el "Informe Cadbury" [19] y en los "Principios de Gobierno Corporativo de la OCDE" [19, 36].

Una fortaleza de la presente norma es que está destinada a todas las organizaciones, públicas, privadas, con o sin fines de lucro. También se puede aplicar a empresas de cualquier tamaño, ya que los roles de gobierno pueden coincidir con los gerenciales; proporciona principios guía para los directores de las organizaciones sobre el uso eficaz y eficiente de TI en las mismas, aplicándose al gobierno de los procesos de gestión (y las decisiones) relacionados con los servicios de información y comunicación utilizados por la organización [29]. Estos procesos

podrían ser controlados por los especialistas de TI, por los proveedores externos del servicio o por unidades de negocios dentro de la organización.

El propósito de esta norma es fomentar el uso eficaz, eficiente y aceptable de las TI en todas las organizaciones.

Modelo: los directores ejercerán el buen gobierno de TI a través de tres tareas principales:

- Evaluar el uso actual y futuro de las TI.
- Dirigir la preparación e implantación de los planes y las políticas para garantizar que el uso de las TI satisface los objetivos del negocio.
- Supervisar la conformidad con las políticas y el desempeño frente a los planes.

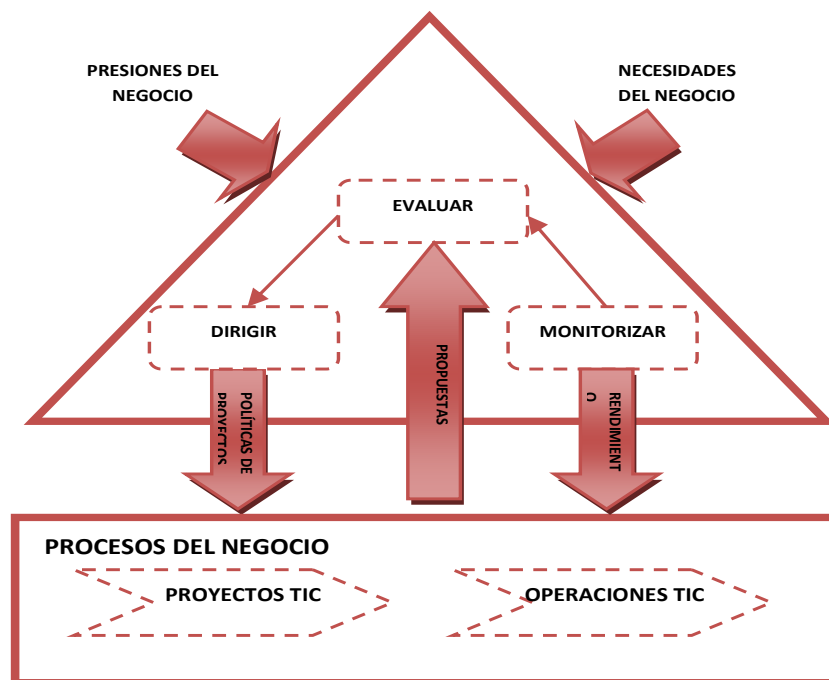


Figura 5 MODELO DE BUEN GOBIERNO CORPORATIVO DE TI. TOMADO DE [35]

En la Figura 5 se muestra el modelo de buen gobierno de TI, el cual consta del ciclo "evaluar, dirigir, monitorear" el cual se aplica a cada uno de los 6 principios de buen gobierno que define la norma y que se detallan a continuación.

Para comprender el modelo anterior, se debe seguir el "ciclo de gobernanza" [29]:

- Gestión del negocio, como parte de su responsabilidad en los procesos de negocio, prepara propuestas para el uso de TI;
- Las propuestas son evaluadas por el Gobierno Corporativo, teniendo debidamente en cuenta las presiones comerciales y las necesidades del negocio;
- Sobre la base de su evaluación, los órganos del Gobierno Corporativo dirigen a los directores del negocio en las acciones específicas;
- El Gobierno Corporativo dirige a los directores según los planes y las políticas aprobadas;

- La Gerencia Corporativa de Proyectos se compromete a proporcionar la capacidad requerida a la organización;
- Dichas capacidades, como operaciones de TI, se utilizan para operar el negocio;
- El rendimiento de las TI y de la gestión empresarial en conformidad con las normas y políticas, se informa periódicamente al Gobierno Corporativo;
- El órgano de Gobernanza Corporativa supervisa los informes para evaluar el rendimiento y la conformidad. El conocimiento en la organización de la vigilancia en el rendimiento hace que las propuestas se evalúen con mayor detenimiento.

2.4.3. MARCO DE GOBERNANZA DE TI: CALDER – MOIR

El marco de gobernanza de TI que se presenta está íntimamente relacionado con la norma ISO/IEC 38500:2015 [8] y su finalidad es la de proporcionar una guía a aquellos involucrados en la toma de decisiones (Junta directiva, Ejecutivos, Profesionales de TI entre otros). Se propone responder las dos preguntas claves de la gobernanza: ¿Estamos haciendo lo correcto? ¿Lo hacemos eficientemente? Para responderlas Alan Calder [9] define un marco dividido en seis segmentos y cada uno de ellos en tres capas.

El marco incluye el ciclo evaluar, dirigir y monitorear que propone el estándar ISO/IEC 38500 [8] aplicado entre las capas de cada uno de los segmentos, estableciendo así los niveles de responsabilidad que existen entre los mismos y contribuyendo a implementar la gobernanza. También incorpora el ciclo de calidad: planificar, hacer, verificar y actuar a diferentes niveles intra e inter-segmentos.

En la siguiente tabla (Tabla 1) se muestra la correspondencia directa entre los segmentos del marco y los principios que expresa la norma ISO/IEC 38500 [8]. Como puede apreciarse existe una correspondencia total entre ambos.

		Marco de Gobernanza de IT					
		Estrategia del negocio	Riesgo, Conformidad	Estrategia de TI	Cambio	Balance de TI	Operaciones
ISO/IEC 38500	Principio	Responsabilidad					
		Estrategia					
		Adquisición					
		Desempeño					
		Conformidad					
		Factores humanos					

Tabla 1 Correspondencia entre el marco Calder-Moir y la norma ISO/IEC 38500 [8].
Adaptado de [37]

2.4.4. *MARCOS DE GESTIÓN DE TI*

La mayor parte de los marcos existentes son relativos a la gestión de TI, en particular, se ha puesto énfasis en los aspectos relacionados con el suministro por parte de TI al negocio ya que dichos marcos han sido elaborados para especialistas de TI. Poco se ha escrito desde el punto de vista del negocio y de lo que el mismo demanda a TI, elemento fundamental, particularmente en empresas medianas y pequeñas, donde la formación de los responsables del negocio es en general, escasa [29].

El marco CobiT© 5

El IT Governance Institute e ISACA, publicaron en Abril de 2012, la versión 5 del marco COBIT (Control Objectives for Information and related Technology) [5]. Esta nueva versión integra y actualiza los marcos CobIT 4.1 [4], Val IT 2.0 [6] y Risk IT [11] haciéndolo ISO/IEC 38500 compatible.

Su principal objetivo es proporcionar un marco que ayude a las empresas a alcanzar sus objetivos acerca de la gestión de TI, es decir el valor óptimo de sus inversiones en TI manteniendo un equilibrio entre la obtención de beneficios, los niveles de riesgo aceptables a la organización y el uso de los recursos.

La premisa sobre la que se basa es que los negocios necesitan información confiable para alcanzar sus objetivos, por lo que las empresas estarán dispuestas a invertir en recursos para que los procesos de TI ofrezcan la información que la empresa necesita para alcanzar dicho éxito [38]. COBIT© 5 [5] proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio, permite el desarrollo de políticas y buenas prácticas para el control de las tecnologías en toda la organización, enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio. Se basa en cinco principios clave para la gobernanza y la gestión de TI:

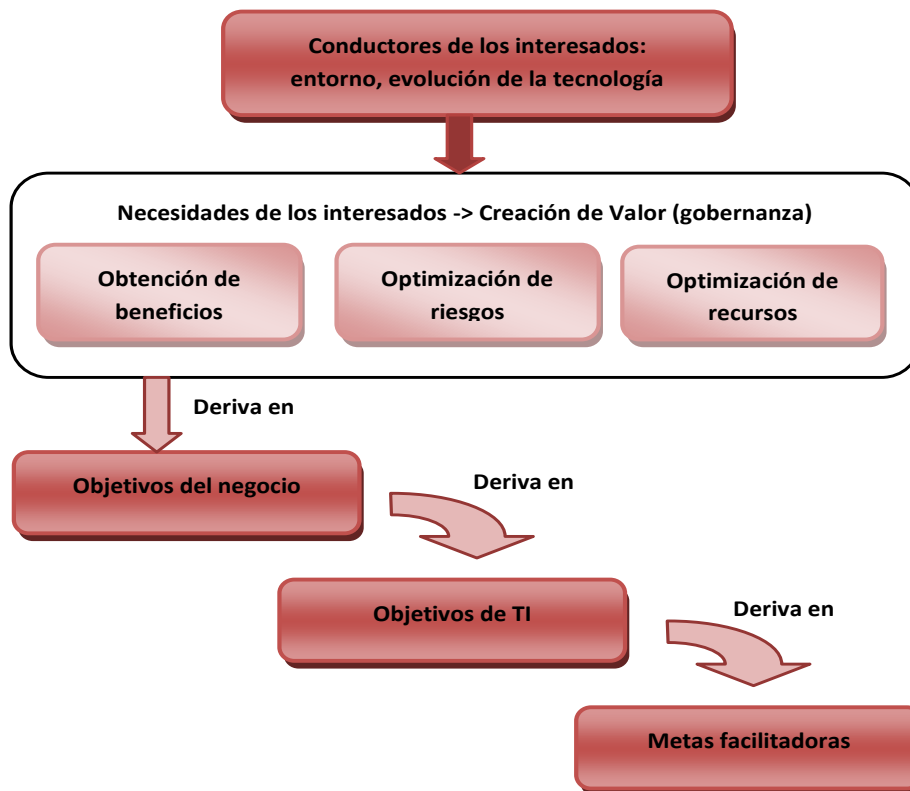


Figura 6 OBJETIVO DE LA GOBERNANZA. TOMADO DE [5]

- Principio 1: Satisfacer las necesidades de las partes interesadas
- Principio 2: Abarca toda la organización de "extremo a extremo"
- Principio 3: La aplicación de un marco único e integrado
- Principio 4: Proporciona un enfoque holístico de la gobernanza
- Principio 5: Diferenciación entre gobernanza y gestión

En conjunto, estos cinco principios permiten a la empresa construir un buen gobierno de TI y un marco de gestión que optimiza la información y la inversión en tecnología para el beneficio de las partes interesadas.

CobIT 5 [5] define el siguiente modelo de madurez de 6 niveles (nivel 0 a nivel 5):

- 1) Incompleto: el proceso es inexistente o incompleto o falla en la implementación de su cometido.
- 2) Realizado: el proceso alcanza su objetivo.
- 3) Gestionado: el proceso es implementado de forma que se pueda gestionar (planificar, monitorear y ajustar), los productos resultantes de la aplicación del proceso son controlados y mantenidos.
- 4) Establecido: el proceso se implanta de acuerdo a un proceso definido.
- 5) Predecible: el proceso que se ha implementado de acuerdo a un proceso definido, ahora opera dentro de límites establecidos.
- 6) Optimizado: el proceso está bajo un sistema de mejora continua.

Cada nivel es alcanzado cuando se cumplen todas las prácticas relativas al mismo y en consecuencia las relativas a los niveles anteriores.

Experiencia en Risk IT

De una experiencia personal del autor en el mundo de las tecnologías de la información, en la pequeña y mediana empresa (PYME), se pone de manifiesto el riesgo inherente a la aplicación de estas tecnologías en el quehacer diario de la empresa.

Siempre que el departamento de las TI, dentro de la pequeña y mediana empresa, se encuentra con obstáculos, debidos a las limitaciones propias del paso del tiempo, a la antigüedad de los equipos, a los cambios de personal, creación de nuevos productos, estrategias o crecimiento de la empresa, se pone de manifiesto el hacer una parada en el tiempo y plantear un nuevo proyecto a futuro que garantice las limitaciones presentes y futuras para la eliminación de los riesgos. Se plantea hacer una Gestión Integral del Riesgo (ERM) y poner en marcha una serie de herramientas para su implantación. En el [Anexo VIII] se presenta el trabajo realizado y los resultados obtenidos del mismo.

ITIL v. 3 - Information Technology Infrastructure Library

ITIL [7] surge a finales de la década de 1980, como respuesta a una necesidad del Gobierno Británico de estructurar sus organizaciones de TI. Esto dio lugar a un conjunto de conceptos y mejores prácticas en la Administración de Servicios de TI (ITSM, sus siglas en inglés), y a una descripción detallada para la implementación de las mismas [7,39].

Los objetivos en el desarrollo de la Biblioteca de Infraestructura de TI fueron:

- *facilitar la gestión de la calidad de los servicios de TI.*
- *aumentar la eficiencia con la que los objetivos de la empresa se cumplan.*
- *mejorar la eficiencia, aumentar la eficacia y reducir los riesgos.*
- *proporcionar los códigos de prácticas en apoyo de la calidad total.*

La Administración de Servicios de TI se refiere a la planificación, suministro, diseño, implementación, operación, apoyo y mejora de los servicios de TI que satisfagan las necesidades del negocio.

Originalmente creada como una colección de libros, cada uno de los cuales cubría un área específica, ITIL[7] se construyó utilizando el modelo de procesos de control y administración de las operaciones atribuido a Edwards Deming [31] y a su ciclo Plan-Do-Check-Act (PDCA)[32,33].

ITIL [7] ha pasado por varios procesos de revisión, actualización y consolidación, *en su última versión el desarrollo más significativo ha sido la evolución desde un marco de trabajo basado en procesos a una estructura integral que refleja el ciclo de vida de los servicios de TI.*

Existen numerosos estudios realizados [40] en los que se integra ITIL [7] con marcos como CobIT [4], Val IT [7] , ISO 27000 [41], entre otros, así como la integración que realiza el marco Calder-Moir [9] donde como herramienta de gestión de servicios se incorpora ITIL [7].

El Cuadro de Mando Integral aplicado a la Gobernanza de TI

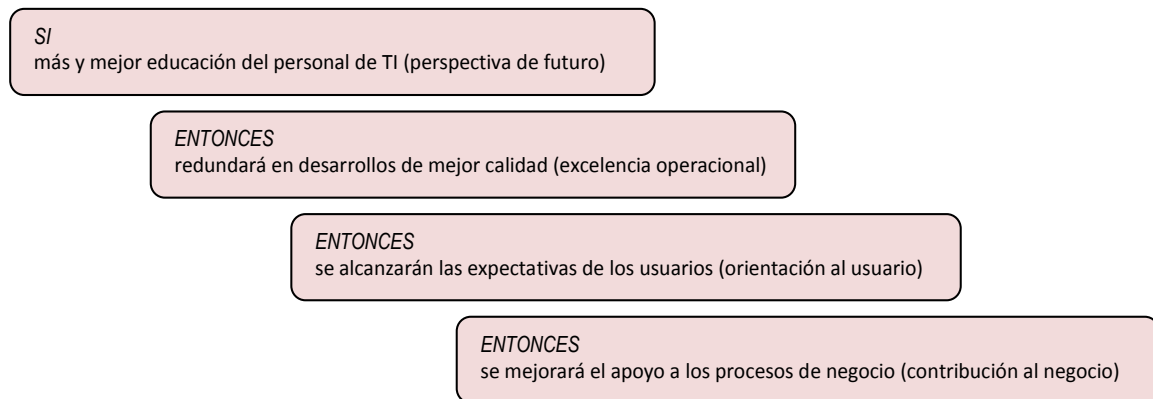


Figura 7 RELACIONES CAUSA EFECTO. ADAPTADO DE [43]

El Cuadro de Mando Integral (Balanced Scorecard - BSC), inicialmente desarrollado por Kaplan y Norton [42], es un sistema de gestión del rendimiento, que permite a las empresas dirigir sus estrategias de medición y seguimiento. Este sistema se ha aplicado a las tecnologías de la información (TI) integrando el BSC del negocio con el de TI (IT BSC), de esta manera se apoya la alineación entre ambos [43]. Para lograr lo anterior, las cuatro perspectivas del BSC del negocio deben ser trasladadas para ser aplicadas en el entorno de TI [44].

A continuación se enumeran los elementos de un BSC de TI estándar [45]. Existen cuatro perspectivas, la de orientación del usuario, la de excelencia operativa, la perspectiva de proyección futura y la perspectiva de contribución al negocio. Para cada una de estas perspectivas se deben definir indicadores y métricas, se harán evaluaciones periódicas. Se deben establecer las relaciones de causa-efecto y las conexiones entre las métricas y los indicadores de rendimiento. Estas relaciones de causa-efecto tienen que ser definidas a través del cuadro de puntuación total (Figura 7).

EL IT BSC se vincula con el negocio a través de la perspectiva de contribución al mismo, en la figura 8 se muestra el vínculo entre ambos integrando los distintos niveles de cuadro de mando.

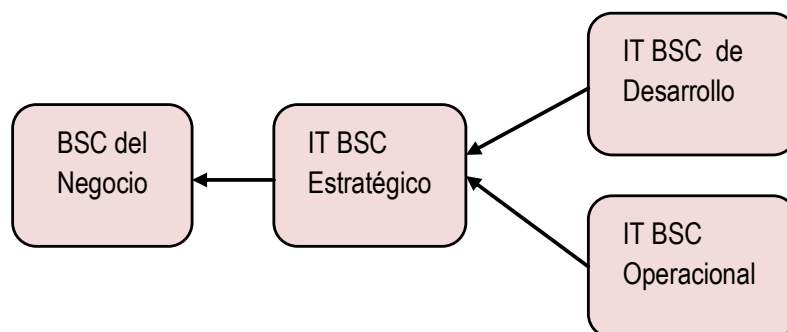


Figura 8 CASCADA DE CUADROS DE MANDO. ADAPTADO DE [43]

La propuesta de Van Grembergen [43, 45] acerca de cómo el BSC contribuye a la gobernanza de TI está relacionada con la cascada de cuadros de mando ya que se fusionan el BSC del negocio con los de TI.

2.5. Buen Gobierno de TI

Un buen Gobierno de TI debe tener un sistema en el cual todos los involucrados, incluyendo a los miembros de la Alta Gerencia, empleados y responsables de los demás departamentos de la compañía tengan el input necesario en el proceso de toma de decisiones. Esto previene el divorcio entre objetivos de TI y objetivos de negocio. Además previene que usuarios críticos de los servicios TI protesten por no tener un sistema que rinda según sus expectativas.

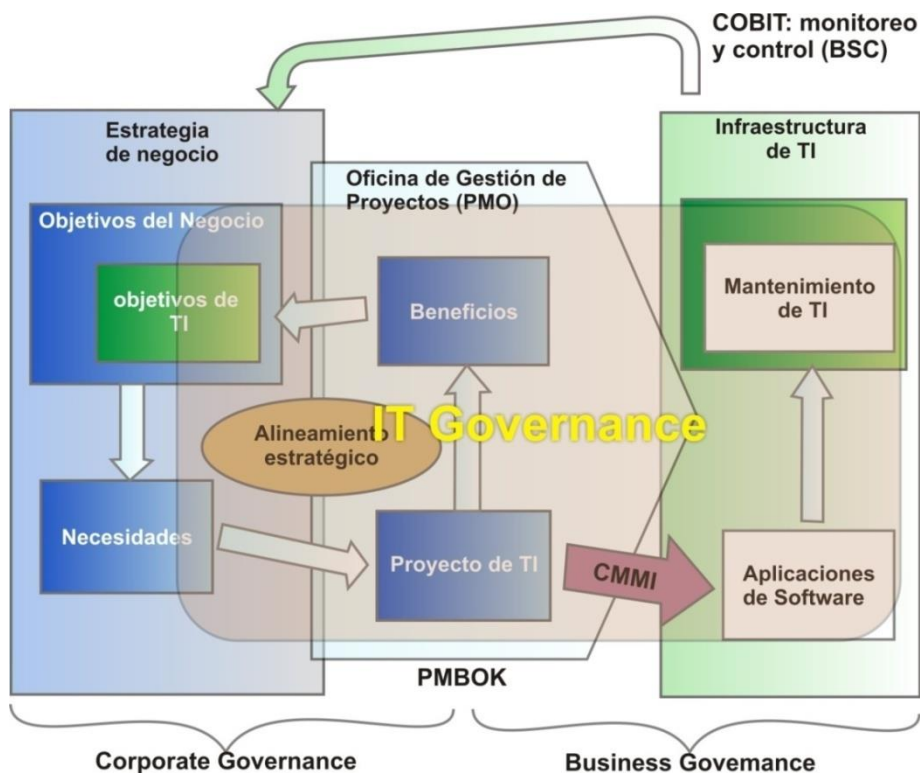


Figura 9 Información de interés del mundo TI [online] [15 junio 2010]. Disponible en Internet :<<http://www.helkyncoello.wordpress.com>>

Podemos decir que un buen gobierno de TI:

- Es un proceso.
- Asegura la obtención de los beneficios esperados de las TI.
- Mediante el uso de los recursos de TI.
- Que involucren planes que soporten a la organización.
- Para acrecentar el éxito sostenido de la misma.

Se recalca entonces al buen Gobierno de TI como un proceso para obtener beneficios que incrementen el éxito de la compañía, usando la infraestructura de TI adecuada con los planes y proyectos adecuados.

El Gobierno de TI efectivo alienta y eleva la capacidad de la gente de las empresas en el uso de TI y asegura el cumplimiento de la visión general y los valores de la empresa. La buena definición de los procesos del Gobierno de TI por parte de los ejecutivos empresariales así como de las unidades de TI es de suma importancia en cuanto al valor que la empresa recibe de TI.

Un buen Gobierno de TI es crítico para asegurar que las decisiones de TI estén alineadas a los objetivos de la compañía.

En la industria de TI, las compañías con buenas prácticas de Gobierno de TI obtienen 20% más en retornos de los activos que aquellas empresas con un Gobierno de TI débil. [28]

Un buen Gobierno de TI armoniza las decisiones sobre el manejo y el uso de con las conductas deseadas y los objetivos empresariales.

Sin estructuras de gobierno cuidadosamente diseñadas e implementadas, las empresas dejan dicha armonía al azar. Hay muchas razones por las cuales las decisiones de TI no deben ser dejadas a la suerte, y por ende se necesita buen gobierno.

2.5.1. *OBJETIVOS DEL BUEN GOBIERNO DE TI*

Como analizamos anteriormente la expectativa principal está en la generación de valor, lo cual es responsabilidad primordial de los ejecutivos y accionistas, representados por la dirección. Son estos directivos quienes conducen la estrategia de las TI y de la empresa, y quienes deben comprender que un manejo adecuado de la infraestructura de las TI de la organización, como parte integral del manejo de una empresa, es la única manera de lograr la generación de este valor.

Para lograr esta generación de valor, debe asegurarse que las iniciativas de TI tengan un desempeño adecuado (helkyncoello.wordpress.com) que cumpla los siguientes objetivos:

- Que las TI estén alineada con la empresa y produzcan los beneficios prometidos.
- Que las TI habiliten a la empresa al explotar oportunidades y generar los máximos beneficios.
- Que los recursos de la TI se empleen responsablemente.
- Que los riesgos relacionados con la TI se manejen adecuadamente.

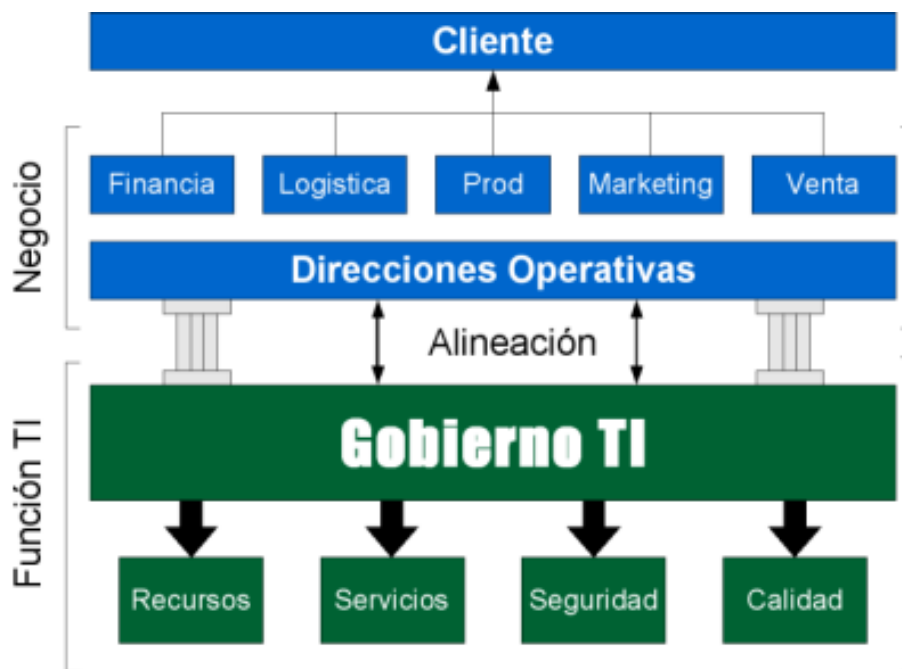


Figura 10 El gobierno TI garantiza la alineación de la función TI con las necesidades de su negocio. Gobierno de TI [online] [17 junio 2010]. Disponible en Internet :<<http://www.agaex.com> >

Una forma de hacer una rápida auto-valoración respecto a la aplicación del buen Gobierno de TI y la entrega de valor a la que éste conlleva es haciendo cuatro preguntas claves.

La primera pregunta es: “**¿Estamos haciendo lo correcto?**”, y tiene un sentido de verificación de que tan alineadas se encuentran las TI de la organización con la estrategia de negocios. Una respuesta satisfactoria a esta pregunta demuestra el alto grado de cohesión entre TI y negocios.

La segunda y tercera pregunta para esta auto-valoración sería: “**¿Lo estamos haciendo de la manera correcta?**” y “**¿Lo estamos haciendo bien?**”. Estas dos preguntas presuponen que existen mecanismos por los cuales se verifica y controla no solo el output final sino también el proceso de creación de dicho output (el proceso).

Finalmente, la última pregunta que puede hacerse es la siguiente: “**¿Estamos obteniendo los resultados esperados?**”, lo que implica un análisis para determinar si hay un retorno de inversión adecuado respecto a las iniciativas de TI realizadas.

A continuación, se muestra de manera gráfica estas cuatro preguntas dentro de un círculo iterativo de auto-valoración, indispensable para lograr una mejora continua.

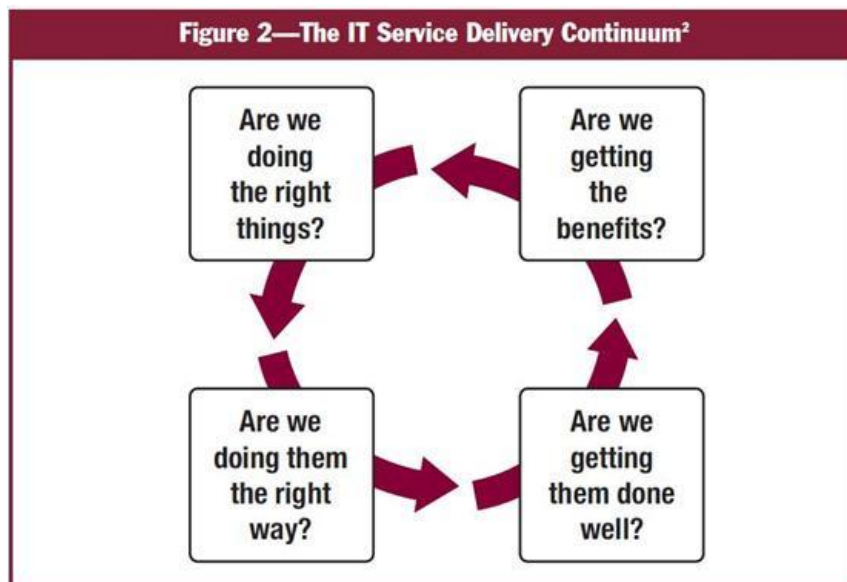


Figura 11 Información de interés del mundo TI [online] [15 junio 2010].
 Disponible en Internet :<<http://www.helkyncoello.wordpress.com>>

2.5.2. *DOMINIOS DEL BUEN GOBIERNO DE TI*

Expondremos las dimensiones sobre las cuales gira un Buen Gobierno de TI:

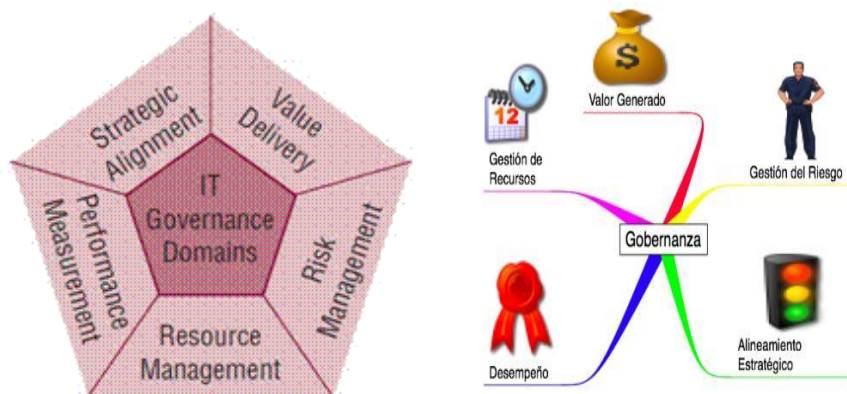


Figura 12 Información de interés del mundo TI [online] [15 junio 2010].
 Disponible en Internet :<http://www.helkyncoello.wordpress.com>

- Alineamiento Estratégico.
- Entrega de valor.
- Manejo de riesgos.
- Gestión de recursos.
- Control y monitorización. Medición de rendimiento.

Mientras más alta sea la jerarquía de la medición de los objetivos, más se desvanecerá el valor (es decir, menor será la influencia que el manejo de TI pueda ejercer). Esto significa que medir el impacto de una inversión en TI es mucho más fácil en la parte inferior de la jerarquía de la organización que en la parte superior de la misma.

2.5.3. *GOBIERNO DE TI VS GESTIÓN Y CONTROL DE TI*

El Gobierno de las TI usualmente se confunde con marcos de trabajo de buenas prácticas de administración y control de TI. La ISO 38500 [8] ha ayudado a clarificar esta confusión describiendo el buen Gobierno de TI como el sistema de gestión usado por la Alta Dirección. En otras palabras, el buen Gobierno de TI trata acerca de la administración de los recursos de TI para satisfacer a los involucrados, quienes esperan un retorno de su inversión. Los responsables de esta administración mirarán a la Alta Gerencia para implementar los sistemas y controles de TI necesarios para lograr dicho retorno de inversión.

Por otro lado, los marcos de trabajo de gestión y control de TI brindan modelos para la gestión de riesgos y control de objetivos, que si bien es cierto, son componentes esenciales de un buen Gobierno de TI, es mucho más importante para dicho Gobierno de TI enfocarse en la entrega de valor. [18]

Beneficios de un buen Gobierno de TI

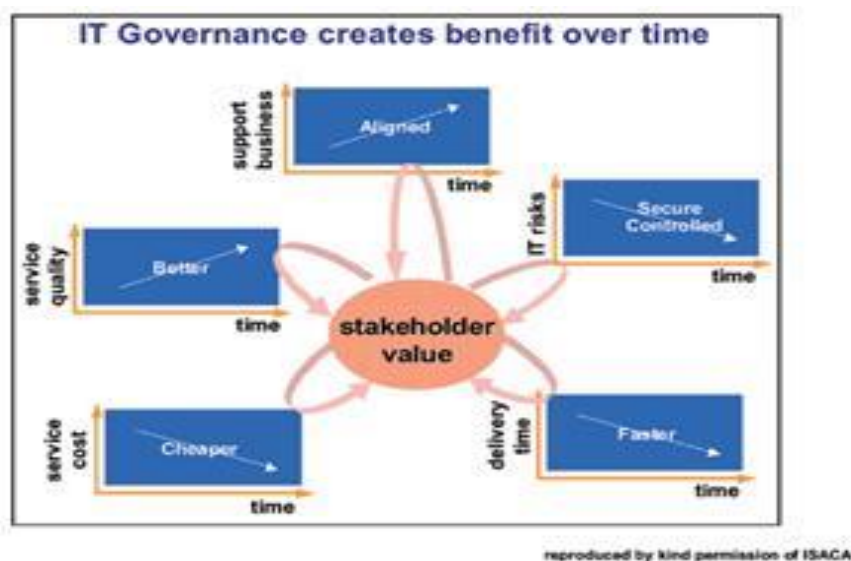


Figura 13 Información de interés del mundo TI [online] [15 junio 2010].

Disponible en Internet :<http://www.helkyncoello.wordpress.com>

Los beneficios que un Buen Gobierno de TI proporciona están íntimamente relacionados a las dimensiones que éste abarca:

- Mayor alineamiento estratégico
- Menores riesgos
- Mejor calidad de los servicios TI
- Menores costes
- Menores tiempos de entrega y respuesta

2.6. Gobernanza de TI en PyMEs

De acuerdo con Samuwai [46], para las economías en desarrollo, las inversiones en TI son un elemento crítico de crecimiento, de desarrollo y de modernización de la sociedad, en particular por estar formadas mayoritariamente por pequeñas y medianas empresas. En particular la realidad del mercado industrial en el Uruguay hace que las empresas categorizadas como PyMEs tengan una incidencia fundamental; según la DINAPYME a datos del 2011 el 99% de las unidades económicas productivas del sector privado del Uruguay son PyMEs y el 70% de las personas trabaja en empresas tipificadas como tales. Esta particularidad hace que sea altamente relevante analizar elementos de gobierno de TI aplicados a este tipo de empresas. Éste tipo de empresa aporta el 33% de PBI y el 25% de la inversión.

Estadísticas de la SBA de Estados Unidos [16] muestran que en el 2007 las pequeñas empresas generaron alrededor del 50% de todas las ventas estadounidenses, y también contribuyeron al 50 % del PBI privado. Además, emplearon a más del 50% de la fuerza laboral de ese país.

Para Gartner [47] la evidencia indica que las inversiones globales en TI serán mayores al 5%, siendo una parte importante de dicha inversión canalizada hacia economías en desarrollo, las cuales están lideradas principalmente por empresas PyMEs. La información es un bien en sí mismo que debe ser valorado y posee vital importancia tanto en empresas pequeñas, medianas o grandes.

Según Heeks [48], los errores en las inversiones relacionadas con tecnología son mayores en las economías en desarrollo, la evidencia indica que el 35% de las inversiones en TI en éstas economías se traducirá en valor, mientras que el 50% fallará parcialmente. Para Samuwai [46], los factores que determinan estos fracasos son la falta de gobernanza de TI, regulaciones externas débiles así como la corrupción, la escasez de mano de obra especializada y la inestabilidad política entre otros.

Una visión de las PyMEs que ya Raymond [49] en el año 1985 (citando a Welsh y White) afirmaba, es que "A small business is not a little big business" por lo que las soluciones que se aplican a las grandes organizaciones no pueden aplicarse a escala en las pequeñas, sino que se deben diseñar marcos que contemplen las características propias que poseen las PyMEs.

2.6.1. *ALINEAMIENTO ESTRATÉGICO DE TI EN PYMES DEL URUGUAY*

Dada la singularidad encontrada en la gobernanza de TI en PyMEs con respecto a grandes empresas, tomamos el trabajo de tesis de maestría "Análisis del alineamiento estratégico de TI en PyMEs del Uruguay" [50] donde se desarrolló un modelo de madurez para medir el alineamiento de los objetivos de TI con los objetivos estratégicos de las PYMES, que aplica específicamente la mejora en la gestión de TI y aplica a este tipo de empresas.

Este modelo se compone, a semejanza de los modelos de madurez más conocidos (COBIT [4], ValIT [6], CMM [51], etc.) de una escala ascendente con cinco niveles de madurez. Cada nivel representa un modelo de empresa PYME con determinados atributos de madurez en

diferentes áreas de TI. Cada nivel del modelo contiene implícitamente los atributos del nivel inmediato anterior.

En el modelo, los niveles se representan en filas de una matriz de atributos, comenzando por el nivel uno y llegando hasta el nivel cinco. Se identificaron las siguientes seis áreas, que se representan en columnas de la matriz, como objetivos estratégicos de la organización.

- Estructura de TI
- Valor de TI
- Servicios de TI
- Riesgos y Seguridad de TI
- Toma de Decisiones
- Gobierno de TI

El modelo plantea que una de las áreas a tener en cuenta son los Riesgos y Seguridad en TI el cual es tratado especialmente en el presente trabajo donde se desarrolla e implementa un marco de buenas prácticas para la gestión de riesgos en empresas de tipo PyMEs en la República Oriental del Uruguay.

2.6.2. RIESGO DESDE EL PUNTO DE VISTA DE LA GESTIÓN DEL CONOCIMIENTO

El riesgo se puede mitigar, transferir, aceptar y evitar [1] para lo cual se requiere conciencia de riesgo por parte de los directores superiores de la empresa, entendimiento del apetito del riesgo de la empresa, transparencia sobre los riesgos significativos de la empresa e implementar las responsabilidades de la administración de riesgos dentro de la organización.

Se definen así las siguientes 4 variables a tener en cuenta en la gestión del riesgo:

- 1) Grado de Conciencia de riesgo por parte de los directores de la empresa.
- 2) Entendimiento del apetito de riesgo de la empresa.
- 3) Transparencia sobre los riesgos significativos de la empresa.
- 4) Nivel de compromiso de la alta dirección en la implementación de las responsabilidades de la administración de riesgos dentro de la organización.

Riesgos desde el punto de vista de los procesos de Gestión del conocimiento.

De esta forma contemplando las variables anteriores, se identifican las siguientes variables con una visión desde la gestión del conocimiento, con lo que tenemos:

- Grado de definición de conocimientos, habilidades y capacidades alineados a la estrategia del negocio.
- Grado de identificación de conocimientos que son estratégicos para la organización.
- Grado de incorporación del conocimiento y la experiencia en la organización.

- Grado de preservación del conocimiento en la organización.
- Grado de diseminación del conocimiento en la organización.
- Grado de aplicación y utilización del conocimiento en la organización.
- Existencia de innovación.

El [Anexo XIII] detalla cada una de estas variables y su justificación.

2.7. Definición de Conocimiento

Existen diversas definiciones acerca de lo que se entiende por conocimiento. Según [52] el conocimiento es una mezcla fluída de experiencia estructurada, valores, información contextualizada y discernimiento experto que provee un marco de referencia para evaluar e incorporar nuevas experiencias e informaciones.

El conocimiento es todo el cúmulo de aprendizajes y habilidades que los individuos utilizan para solucionar problemas [53]. Hablando en forma abstracta los conocimientos constan de descripciones, relaciones y procedimientos en algún dominio de interés [54]. La distinción entre conocimiento e información, así como la distinción entre información y datos permitirá comprender mejor el concepto de conocimiento.

Según [55] los datos pueden ser números, palabras o imágenes para los cuales no se ha especificado un contexto de significación o una organización. Para que los datos se conviertan en información deben ser presentados en un contexto, con algún propósito y con una organización discernible de modo que tengan relevancia para una situación, problema o condición. El conocimiento es subsecuentemente aplicado para interpretar la información disponible sobre una situación en particular y para decidir cómo manejarla. El conocimiento es lo que se usa para determinar el significado de una situación o condición.

La distinción efectiva entre información y conocimiento no se encuentra en el contenido, estructura o utilidad de la supuesta información o conocimiento sino que conocimiento es información procesada por las mentes de los individuos; es información personalizada relativa a hechos, procedimientos, conceptos, ideas y juicios [56].

2.7.1. PROPIEDADES DEL CONOCIMIENTO

Los conocimientos tienen una serie de propiedades y características particulares que están ausentes en los demás recursos de las instituciones así como en los recursos tradicionales como la tierra y el capital. Entre las propiedades cabe distinguir las siguientes [57] - [58]:

- Son intangibles y difíciles de medir. Se les evalúa como activos y sólo se les conoce por los efectos que producen.
- Son volátiles; esto significa que pueden estar en un momento y al siguiente ya no estar, es decir se pueden fugar con rapidez.

- La mayoría de las veces están incorporados en agentes con voluntad, en particular en seres humanos.
- A diferencia de cualquier otro recurso no se consumen por su uso, sino se incrementan mediante el uso. Uno puede dar recursos sin que el donante los pierda.
- Su presencia significa poder para las organizaciones. Tienen un alto grado de impacto sobre las mismas.
- Con frecuencia hay que esperar a que estén disponibles. No pueden comprarse en el mercado en cualquier momento.
- Tienen el don de ubicuidad. Pueden usarse por distintos procesos al mismo tiempo.
- Son abundantes y crecen de modo exponencial, o casi. Cuanto más se conoce y se ha inventado, más fácil resulta conocer e inventar más.
- No tienen límites en cuanto a modos, formas, espacio o cantidad. Previsiblemente no existe un límite superior a ese crecimiento de los conocimientos y las invenciones.
- El crecimiento de los conocimientos es virtualmente irreversible. Si bien es posible ignorar algunas cosas, y olvidar otras, una vez que algo es conocido, es prácticamente imposible desconocerlo. De la misma manera, una vez que se ha inventado algo, es imposible evitar su invención.
- Al iniciarse los conocimientos en la mente humana y ser un resultado directo del cerebro humano, sus materiales están muy elaborados e influenciados por percepciones, vivencias, experiencia y conocimientos previos que serán traducidos en símbolos, guarismos o ecuaciones formales, es decir, en procedimientos de consulta y acción de alta calidad y sutileza, lo que puede dar lugar a una impregnación ideológica del contenido transmitido.
- Los conocimientos se auto-alimentan. Esto significa que cuanto más conocimiento se tiene más se obtiene. Este principio también rige en el terreno de las publicaciones científicas y fue postulado por R.K. Morten [59].

2.7.2. *GESTIÓN DEL CONOCIMIENTO*

Asociado al concepto de conocimiento está el aprendizaje y la experiencia, existiendo una relación muy estrecha y vinculante entre estos conceptos. Existen dos tipos de conocimiento, el tácito y el explícito.

El tácito es difícil de formalizar y de articular, es el conocimiento implícito. Reside en las mentes de las personas. Se adquiere principalmente a través de la práctica y la experiencia, y se expresa en las acciones humanas en las formas de evaluaciones, actitudes, puntos de vista, motivaciones y juicios [60].

El conocimiento explícito puede transmitirse utilizando el lenguaje formal y sistemático, y que puede ser o ha sido capturado y codificado en manuales, libros, procedimientos y reglas.

Podemos definir la gestión del conocimiento como la colección de procesos que gobiernan la creación, diseminación, y utilización de conocimiento [61].

Es el proceso sistemático y organizacionalmente especificado para adquirir, organizar y comunicar tanto el conocimiento tácito como el explícito de los empleados, de modo que otros empleados puedan hacer uso de él para ser más efectivos y productivos en sus trabajos [62].

La gestión del conocimiento implica cualquier proceso o práctica para crear, adquirir, capturar, compartir y usar conocimiento, cualquiera sea el lugar donde resida, para mejorar el aprendizaje y el desempeño en las organizaciones [63].

Según [57], la gestión del conocimiento puede considerarse como el proceso de: integrar la información, extraer sentido de información completa, renovar la información.

De esta manera se puede comenzar una iniciativa de gestión del conocimiento realizando los siguientes pasos [57]: integrar la información procedente de múltiples fuentes, crear múltiples caminos para realizar conexiones persona a persona y persona a información y viceversa, explotar todas y cada una de las formas de establecer conexiones (sistemática, auto-selección, aleatoria o cualquier combinación de ellas).

La gestión de conocimientos tiene los siguientes objetivos [57]: hacer que las instituciones en general y las empresas en particular actúen tan inteligentemente como sea posible para asegurar su viabilidad y su éxito global y en otro caso, darse cuenta del mejor valor de sus activos de conocimientos.

Según [57] para alcanzar estas metas las organizaciones avanzadas, construyen, transforman, organizan, despliegan y usan efectivamente activos de conocimientos siendo el propósito general de la gestión del conocimiento el maximizar la efectividad y el retorno de la empresa relacionados con los conocimientos de sus activos de conocimientos y renovarlos constantemente. De esta manera se posibilita el bienestar y la viabilidad a largo plazo de la empresa.

La gestión del conocimiento gestiona los procesos efectivos de conocimiento entendiendo y centrándose en la gestión sistemática, explícita y deliberada, construcción, renovación y aplicación de conocimientos [57].

La gestión del conocimiento requiere de la coordinación activa de varias actividades, activos y otros factores dentro de una organización.

2.7.3. *HISTORIA DE LA GESTIÓN DEL CONOCIMIENTO*

El desarrollo del conocimiento y su capacidad, la generación, administración, almacenamiento y distribución del mismo datan desde épocas muy remotas [57].

Los conocimientos han sido gestionados implícitamente desde las primeras actividades laborales de supervivencia como la preocupación de los cazadores sobre la experiencia y habilidades de sus compañeros de grupo para capturar presas, hasta el aseguramiento de la sucesión de la transferencia en profundidad de los conocimientos por parte de los pueblos sabios a sus futuras generaciones [64].

El proceso de digitalización de la información y su almacenamiento y distribución a través de medios informáticos y telemáticos ha producido una explosión del conocimiento humano que no tiene comparación a otras épocas históricas [57].

Dada la importancia que supone el valor económico del conocimiento aparece la necesidad ineludible de brindar a los usuarios los conocimientos que necesitan, donde los necesiten, como los necesiten y cuando los necesiten, es decir gestionar el conocimiento. Actualmente en el mundo crece cada vez más el interés en las organizaciones por lograr nuevas formas de gestionar el conocimiento con el fin de cumplir eficientemente sus objetivos [57].

Existen determinados autores referentes de la Gestión del Conocimiento como ser Nonaka, Takeuchi, Davenport, Prusak y Probst.

Ikujiro Nonaka e Hirotaka Takeuchi

Estos autores son referentes en el área de la gestión del conocimiento. Realizando trabajos en conjunto. El [Anexo IX] presenta ambos autores así como una breve reseña de sus trabajos.

Thomas Davenport

Es profesor distinguido de Gestión de Tecnologías de la Información en Babson College. También ha sido profesor en la Escuela de Negocios de Harvard, la Universidad de Chicago, en Tuck School of Business de Dartmouth, y la Universidad de Texas en Austin. Ha dirigido centros de investigación de Accenture, McKinsey & Company, Ernst & Young, y CSC. También es Asesor Senior de Deloitte Analytics. Obtuvo su Ph.D. de la Universidad de Harvard, en la ciencia social [64].

En su trabajo con Larry Prusak, definen tres etapas en la gestión del conocimiento a las que denominan Generación, Codificación y Transferencia.

Se debe tener en cuenta que hay muchos factores que no facilitan, retardan o impiden la transferencia del conocimiento imponiendo barreras que pueden ser culturales, falta de confianza y falta de tiempo.

Gilbert Probst

Profesor de Comportamiento Organizacional y Gestión, director del programa de MBA en la Universidad de Ginebra, Suiza. Autor junto a B. Büchel, de *Organizational Learning*, Prentice Hall, Londres, 1996; así como junto a S. Raub y K. Romhardt, de *How to Manage Knowledge*, Gabler, Wiesbaden, 1997. Miembro de Boards of Directors of Kuoni Travel Limited and EPA y presidente de la Board of Swiss Top Executive Training. Es consultor de grandes empresas, incluyendo ABB, Hewlett-Packard, Siemens, Winterthur Seguros y UBS [65].

Plantea la existencia de seis etapas en la gestión del conocimiento a las que llama Identificación, Adquisición, Desarrollo, Compartir o Distribuir el conocimiento, Uso y Retención del conocimiento.

Larry Prusak

Investigador y consultor, fundador y director del Instituto de Gestión del Conocimiento, consorcio mundial de organizaciones dedicadas a la promoción de la práctica de la gestión del conocimiento a través de investigación-acción.

Estudió el conocimiento y el aprendizaje en las organizaciones durante años, con amplia experiencia, tanto en los EE.UU. y a nivel internacional, para ayudar a las organizaciones a gestionar su información y el recurso conocimiento.

Ha trabajado con varias agencias del gobierno de Estados Unidos y ONGs, además de haber impartido clases y conferencias en universidades. Ha publicado varios libros innovadores e influyentes [66].

2.7.4. *PROCESOS DE GESTIÓN DEL CONOCIMIENTO*

A continuación se presentan los procesos que componen la gestión del conocimiento según Probst y Prusak [67]:

Alineación estratégica

Las organizaciones deben alinear los conocimientos, habilidades y capacidades necesarias para poder cumplir eficientemente con la estrategia de negocios definida.

El conocimiento, la experiencia, las habilidades y las competencias que necesita una organización para competir se definen en base a la elección estratégica que esta realiza en relación a diversos factores como la tecnología, los mercados, los productos y los procesos.

Es importante definir los objetivos de conocimiento estratégico en las organizaciones. Estos objetivos definen los conocimientos principales necesarios para la organización, especificando que conocimientos, habilidades y experiencias serán necesarios en el futuro.

Es a través de la estrategia organizacional que se dirige y administra el almacenamiento sistemático de conocimiento y experiencia, tanto individual como colectiva.

Identificación

Consiste en la identificación del conocimiento que es estratégico para la organización. Esto implica la identificación del conjunto de conocimientos, habilidades y experiencias que la organización debe lograr para cumplir con su estrategia de negocios. En este proceso también se identifica el conocimiento que existe en la organización y las brechas de conocimiento entre éste y el conocimiento estratégico.

El identificar los activos de conocimiento implica relevar y construir un inventario de los conocimientos, habilidades y experiencia existentes en la organización. Estos conocimientos y habilidades condicionan lo que la organización puede hacer.

En la identificación de las brechas de conocimiento se analiza la diferencia en relación a la eficiencia y carencias en los conocimientos y experiencia que posee la organización y los que debería poseer para llevar adelante su estrategia de negocios.

También se identifica la brecha estratégica, esto es la diferencia entre lo que la organización debe hacer y lo que la organización puede hacer.

Incorporación

En este proceso se incorpora conocimiento y experiencia en la organización a través de la adquisición de conocimientos desde fuentes externas a la organización o mediante la creación y desarrollo de conocimientos generados internamente. El objetivo es disminuir o eliminar las brechas identificadas en el proceso anterior.

Preservación

Este proceso implica todas las actividades referentes a mantener el conocimiento existente en la organización y asegurar la continuidad del mismo.

En el caso del conocimiento explícito su preservación requiere formalización, codificación, organización y almacenamiento en algún medio. Para lograr la preservación del conocimiento tácito se requiere la permanencia en la organización de los poseedores de ese conocimiento.

Diseminación

Para que el conocimiento pueda ser efectivamente utilizado debe ser distribuido y compartido a través de los diferentes niveles organizacionales.

La diseminación del conocimiento se puede realizar en forma centralizada, decidiendo acerca de que conocimiento distribuir y quienes deben recibirlo para luego difundirlo hacia la organización a través de canales claramente definidos. Esta estrategia se denomina “de empuje”.

También se puede diseminar el conocimiento a través del usuario que accede al mismo según sus necesidades por medio de la estrategia denominada “de extracción”.

Utilización

Este proceso consiste en la aplicación y utilización de las mejores prácticas y las lecciones aprendidas capturadas de proyectos anteriores disponibles en el repositorio de lecciones aprendidas y de mejores prácticas, aplicando y utilizando de esta manera los nuevos conocimientos creados o adquiridos.

2.7.5. *HERRAMIENTAS, TÉCNICAS Y FACTORES*

En las distintas etapas de gestión del conocimiento se aplican herramientas y técnicas para llevar adelante los procesos de gestión del conocimiento.

A continuación se detallan las distintas herramientas y técnicas presentadas por los autores analizados, así como factores que pueden incidir favorablemente o ser obstáculos en dichos procesos:

Herramientas: Accesibilidad, Diseño del área de trabajo, Memoria organizacional, Mapas, Patentes, Benchmarking, Fusión o adquisición de conocimiento, Lecciones aprendidas, Grupos Expertos, Comunidades de práctica, Redes, Mejores prácticas, Análisis de redes sociales.

Técnicas: Cámara web, Videoconferencia, Realidad virtual, Sistemas expertos, Charla informales, Coaching, Mentoring, Bases del Conocimiento, E-learning, Clasificación, Clustering.

Factores: Recursos económicos, Tiempo, Capacitación, Recursos Humanos, Marcos de Buenas Prácticas, Cultura organizacional, CKO, Compromiso de la alta gerencia.

2.7.6. *CREATIVIDAD Y CONOCIMIENTO*

Se define la creatividad como el proceso que lleva a una repentina visión para resolver un problema, basada en la conexión entre dos campos de conocimiento anteriormente separados e independientes.

Es a través de las distintas etapas de creación de conocimiento en espiral, que se habilitan distintas formas de creatividad, generando nuevo conocimiento.

La creatividad permite la innovación y esta la generación de nuevo conocimiento que favorecerá el logro de ventajas competitivas sostenibles. La innovación es vista como la clave fundamental para el beneficio a largo plazo de cualquier organización.

En el artículo [68] se presenta el caso de la organización Unilever donde se plantea que la creatividad puede ser gestionada de forma exitosa, donde se busca satisfacer las necesidades diarias de las personas. Las divisiones de Unilever, Home & Personal Care y Unilever's Bestfoods, proveen jabón en polvo, champú, pasta de dientes, té, helado, ingredientes de cocina, aceites y cremas para consumidores alrededor del mundo. En el año 2002, el balance de Unilever fue de 52 billones de euros, lo cual generó un margen operativo del 14,9% [69].

Unilever tiene una clara meta de dirigir el crecimiento de sus marcas líderes en el mundo mediante una innovación excitante, rápida, y de gran escala. Investigación y desarrollo son el corazón en este proceso.

Como dijo el artista Pablo Picasso *“La creatividad es destrucción, el derribar viejas visiones, nociones, pensamientos o sentimientos a fin de crear algo nuevo”*.

2.7.7. *MAPAS DE CONOCIMIENTO*

Una de las herramientas de gestión del conocimiento que proporciona una orientación visual para gerentes y especialistas a fin de localizar, evaluar o desarrollar el conocimiento en un contexto organizacional, son los mapas de conocimiento que permiten con creatividad generar nuevo conocimiento. Estos condensan la información sobre las fuentes de conocimiento, activos, estructuras, aplicaciones o necesidades de desarrollo.

Los elementos individuales de conocimiento incluidos en dicho mapa pueden ser texto, historias, gráficos, modelos o números.

El mapeo de conocimiento se puede ver como un proceso de asociación de ítems de información o conocimiento (preferentemente en forma visual), de tal manera que el propio mapeo crea conocimiento adicional.

Con el rápido desarrollo de la tecnología de intranet, que permite combinarlos con aplicaciones con acceso a bases de datos, estos podrían llegar a ser un elemento estándar en la gestión del conocimiento de las organizaciones.

A continuación se presenta un ejemplo de mapa de conocimiento para una compañía multimedia:

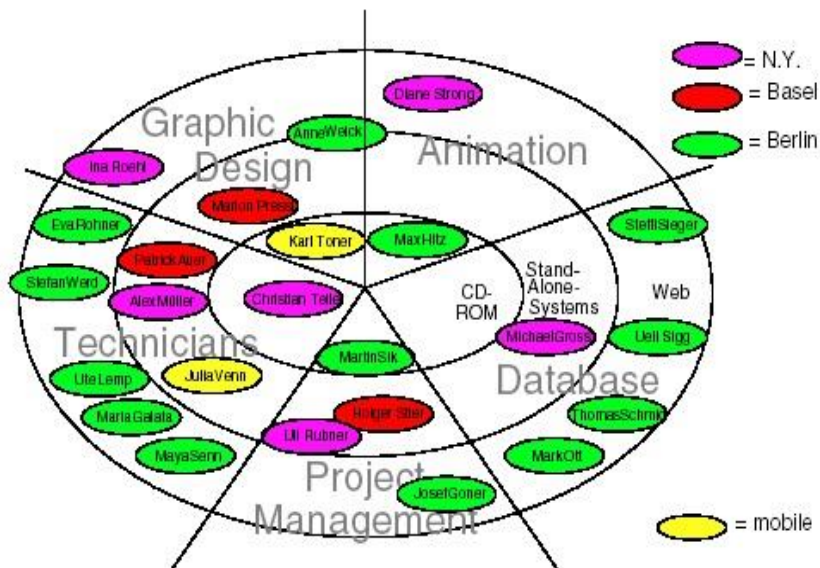


Figura 14 A knowledge source map for a multimedia company (excerpt)

Según [70], se pueden definir 5 tipos de mapas de conocimiento que se pueden utilizar para la gestión del conocimiento organizacional y son: origen, activos, estructuras, aplicaciones y de desarrollo de conocimiento.

2.7.8. ONTOLOGÍAS

Una ontología es una descripción explícita formal de un concepto en un dominio determinado, propiedades de cada concepto describiendo sus características y atributos, así como relaciones entre estas [71]. Una ontología junto a un conjunto de instancias individuales de clases, constituyen una base de conocimiento.

Las clases son el foco de la mayoría de las ontologías. Las clases describen conceptos en el dominio. Una ontología define un vocabulario común para los investigadores que necesitan compartir información en un dominio. Incluye definiciones de los conceptos básicos en el dominio y las relaciones entre ellos de forma tal que puedan ser interpretados por una máquina.

Según [71] se describe una metodología de desarrollo de ontologías para sistemas declarativos basados en marcos. Se hace referencia a los aspectos complejos de la definición de jerarquías de clases y propiedades de clases e instancias, llegando a la conclusión de que no hay una sola ontología correcta para un dominio dado. El diseño de ontologías es un proceso creativo donde dos ontologías diseñadas por personas diferentes no serán iguales. Las aplicaciones potenciales de la ontología y el entendimiento del dominio desde el punto de vista del diseñador, afectarán sin duda las opciones de diseño de la ontología.

Surge así el concepto de Ingeniería Ontológica que corresponde con el conjunto de actividades relacionadas al desarrollo, ciclo de vida, metodologías, herramientas y lenguajes para construir ontologías.

2.7.9. *MARCOS*

Según [72], los marcos son una estructura de datos que representa situaciones estereotipadas construidas en base a experiencias similares ocurridas en el pasado, permitiendo luego aplicar los conocimientos de estas situaciones, eventos y conceptos previos a nuevas situaciones que surjan.

El conocimiento se puede representar por medio de marcos, relaciones, propiedades y facetas [73], donde cada una de ellas se utiliza de la siguiente manera:

- Marcos: para representar conceptos
- Relaciones: para expresar dependencias entre los conceptos
- Propiedades: para describir cada concepto
- Facetas: para expresar de distintas formas los valores que puede tomar cada propiedad

Los marcos pueden ser de 2 tipos: marcos de clase o marcos instanciados. Los marcos de clase representan conceptos, clases o situaciones genéricas y poseen un conjunto de propiedades.

Los marcos instanciados, son utilizados en los dominios de trabajo de los expertos donde existen elementos, instancias o individuos de clases. Por ejemplo, martillo-1 de la clase herramienta para el experto carpintero.

Las propiedades de marcos pueden ser de clase o de instancia, donde las propiedades de clase representan atributos o características genéricas de un concepto o clase. Estas propiedades toman cierto valor en el marco clase, y luego toman siempre el mismo valor en todos los elementos o instancias de la clase. Por otra parte, las propiedades de instancia, en cada instancia toman valores concretos que dependen del elemento de la clase que se esté representando.

Las facetas de las propiedades se clasifican en 3 categorías:

- Facetas que definen propiedades de clase, de instancia y de relación. Las más comunes son: Tipo Ranura, Cardinalidad Mínima, Cardinalidad Máxima y Multivaluada si la propiedad puede tomar más de un valor.
- Faceta que define propiedades de clase y relaciones. Por ejemplo la Propiedad General.
- Facetas que definen propiedades de instancia. Las más comunes son: Valores Permitidos, Valores por Omisión o por defecto.

2.7.10. *REDES SEMÁNTICAS*

Las redes semánticas son otra técnica de representación de conocimientos así como los mapas de conocimiento, donde se expresan conceptos de un dominio y sus relaciones [73].

La información está representada en grafos dirigidos (orientados), donde cada nodo corresponde a un concepto o instancia y los arcos representan relaciones entre estos.

Permiten la visualización gráfica que facilita su entendimiento con una representación intuitiva.

2.7.11. *EDUCCIÓN DEL CONOCIMIENTO*

Dado que los expertos son los que tienen el conocimiento tácito y a su vez presentan dificultad para la explicación de los pasos para la toma de decisiones y como enfrentar problemas (se puede decir que los expertos más competentes son incapaces de describir los conocimientos que usan en resolver los problemas). Los expertos necesitan ayuda externa para explicarse y no necesariamente lo que dicen es exactamente lo que hicieron [55].

Para ello entonces surge el rol del ingeniero en conocimientos.

En base a este planteo, se determina un proceso de educación de conocimiento, el cual sigue un ciclo con etapas de Preparación, Sesión (donde es necesario contar con el experto), Transcripción, Análisis y Evaluación.

Para dicha educación existen variadas técnicas como Entrevistas, Observación, Incidentes críticos, Clasificación de Conceptos, Cuestionarios, Análisis de Protocolos, Emparrillado e Inducción.

El emparrillado es un test de clasificación que permite encontrar conceptos y relaciones, estableciendo prioridades que ayuda en la clasificación.

Depende de la experiencia de quien lo aplica por lo cual es un método subjetivo en cuanto a la clasificación realizada.

2.7.12. *REPRESENTACIÓN INFORMÁTICA DEL CONOCIMIENTO*

Para representar el conocimiento en sistemas informáticos se utilizan entre otros:

- OAV (Objeto – Atributo – Valor) [55]
- Por ejemplo: Objeto : Persona, Atributo : Profesión, Valor : Médico.
- Marcos (presentado anteriormente): donde se manejan conceptos con características y facetas.
- Como ejemplo de implementación se puede ver el software Protege que está basado en marcos.
- Redes

Es interesante establecer una comparación entre las distintas herramientas, resultado de la práctica, donde se puede observar que con Marcos se logra un mayor nivel de detalle en la representación y a su vez, con el uso de OAV se brinda una mayor facilidad de implementación. En relación a la facilidad de interpretación para cada una de estas herramientas tendríamos en orden decreciente de facilidad OAV en primera instancia, seguido de Marcos y por último Redes, y por el contrario tomando en cuenta la facilidad que brindan para representar relaciones, también en orden decreciente de facilidad tendríamos primeramente a las Redes, luego Marcos y finalmente OAV.

2.7.13. CAPITAL INTELECTUAL E INGENIERÍA DEL CONOCIMIENTO

Es la suma de todos los conocimientos de todos los empleados de una empresa que le dan a esta una ventaja competitiva [55]. Estos conocimientos se pueden dividir en Humanos, Estructurales o Relacionales donde se define cada uno de estos como:

- Humanos: hace referencia al conocimiento explícito e implícito, a la capacidad de aprender, al compromiso y experiencia.
- Estructurales: hace referencia al conocimiento estructurado y formalizado.
- Relacionales: hace referencia a las relaciones con el exterior de la empresa.

Por su parte, la Ingeniería del Conocimiento es un conjunto de principios, métodos y herramientas que permiten aplicar el saber científico y de experiencias a la utilización de los conocimientos y sus fuentes [55].

2.8. Chief Knowledge Officer (CKO)

El Gerente del Conocimiento (CKO, por su acrónimo en Inglés de Chief Knowledge Officer), es el principal responsable de la gestión del conocimiento en las organizaciones. Es el encargado de iniciar, impulsar y coordinar los programas de Gestión del Conocimiento.

El [Anexo XI] presenta una descripción de sus características, diferencias con el CIO y la necesidad de dicho rol en la empresa.

2.8.1. ESTRATEGIA DE GESTIÓN DEL CONOCIMIENTO

Según [59], en su estudio sobre gestión del conocimiento en consultoras, existen 2 tipos de estrategias de gestión del conocimiento: de codificación y de personalización. El [Anexo X] presenta un escrito respecto de dicho estudio.

2.8.2. *RELACIÓN ENTRE GESTIÓN DEL CONOCIMIENTO Y GOBIERNO DE TI*

Un buen Gobierno de TI implica una buena gestión del conocimiento y una buena gestión del conocimiento permite un buen Gobierno de TI [18].

Cuanto mejor sea la gestión del conocimiento, experiencia y aprendizaje en una organización, mejor será su Gobierno de TI y cuanto mejor sea el Gobierno de TI en una organización, mejor será la gestión de su conocimiento, experiencias y aprendizaje [18].

El [Anexo XII] presenta un análisis respecto a la relación entre gestión del conocimiento y su influencia sobre el gobierno de TI.

2.8.3. *ANÁLISIS DE LAS ETAPAS A UTILIZAR*

Según la definición de las etapas identificadas en la gestión del conocimiento por los distintos autores que se analizan (Nonaka y Takeuchi, Davenport, Probst), se realiza un mapeo indicando para cada par de etapas, si una contiene a la otra conceptualmente, o si están relacionadas por medio de procesos que pueden aplicar a ambas.

Luego de contar con este mapeo se determinan las relaciones y similitudes entre las etapas de cada autor, para lo cual se agrupan, definiendo así un conjunto reducido que es utilizado en la definición del modelo de gestión del conocimiento aplicado a la gestión del riesgo que se detalla a continuación.

Las etapas definidas por cada autor en base a la cual se realizó el mapeo de la Tabla 2 son las siguientes:

Nonaka y H. Takeuchi

Socialización - Implica la conversión del conocimiento tácito en conocimiento tácito.

Externalización - Implica la conversión del conocimiento tácito en conocimiento explícito.

Internalización - Implica la conversión del conocimiento explícito en conocimiento tácito.

Combinación - Implica la conversión del conocimiento explícito en conocimiento explícito.

Davenport

Generación- Implica actividades para incrementar el stock del conocimiento.

Codificación - Implica poner el conocimiento disponible de forma que sea accesible a quienes lo necesitan.

Transferencia - Implica transmitir el conocimiento.

Probst

Identificación - Implica determinar dónde está el conocimiento. Que es lo que falta conocer.

Adquisición - Implica adquirir el faltante de conocimiento.

Desarrollo - Implica desarrollar nuevas habilidades, productos e ideas

Compartir o Distribuir el conocimiento - Implica intercambiar el conocimiento disponible a quien lo requiera.

Retención del Conocimiento - Implica el almacenamiento y actualización del conocimiento.

Uso - Implica la utilización del conocimiento por quien lo requiera.

Tabla 2. Relaciones entre etapas de los distintos autores (Davenport, Probst, Nonaka y Takeuchi)

	Socialización	Externalización	Internalización	Combinación	Generación	Codificación	Transferencia	Identificación	Adquisición	Desarrollo	Compartir o Distribuir	Uso	Retención
Socialización					2	2	2	2	2	2	2	2	
Externalización					2	2	2	2	2	2	2	2	2
Internalización					2	2	2	2	2	2	2	2	
Combinación					2	2	2	2	2	2	2	2	2
Generación	2	2	2	2					2	2			
Codificación	2	2	2	2							1		
Transferencia	2	2	2	2							2		
Identificación	2	2	2	2									
Adquisición	2	2	2	2	2								
Desarrollo	2	2	2	2	2								
Compartir o Distribuir	2	2	2	2		2	2						
Uso	2	2	2	2									
Retención		2		2									

Referencia:

1 – Etapa indicada en la fila forma parte de la etapa indicada en la columna

2 – Etapa indicada en la fila se relaciona a la etapa indicada en la columna

De esta forma podemos observar una relación entre la etapa de Generación de Davenport con la Adquisición y Desarrollo de Probst, así como la Codificación y Transferencia definidas por Davenport y la etapa de Compartir o Distribuir de Probst.

Se observa que todos los procesos de Socialización, Externalización, Internalización y Combinación de Nonaka y Takeuchi se relacionan con todas las etapas de los restantes autores, salvo el caso de la Retención de Probst, para la cual si consideramos únicamente el caso del conocimiento explícito (ya que hace referencia al almacenamiento del mismo), éste se vincularía con los procesos de Externalización y Combinación únicamente.

De esta forma definimos las siguientes etapas a utilizar en el modelo a definir:

Identificación – Implica determinar dónde está el conocimiento tácito y/o explícito, así como lo que falta conocer.

Generación – Implica actividades para incrementar el conocimiento tácito y/o explícito adquiriendo el faltante de conocimiento o desarrollando nuevas habilidades, productos e ideas.

Codificación, Transferencia, Compartir o Distribuir – Implica codificar, transferir e intercambiar el conocimiento tácito y explícito disponible.

Retención – Implica el almacenamiento y actualización del conocimiento explícito.

Uso – Implica la utilización del conocimiento tácito y/o explícito por quien lo requiera.

3. Marco de Gestión de Riesgos de TI en Función de la Gestión de Conocimiento

3.1. Introducción

La presente tesis plantea la construcción de un marco para la Gestión de Riesgos utilizando como herramienta las propuestas por la Gestión del Conocimiento y un modelo de madurez que permita incorporar en etapas sucesivas el conjunto de buenas prácticas que se detallan en el marco.

En las secciones que se desarrollan a continuación se detallan las matrices a partir de las cuales se vinculan los procesos y dominios que forman el marco de Gestión de Riesgo con las actividades, herramientas y técnicas de Gestión del Conocimiento.

Finalmente se definen roles y responsabilidades dentro de la organización que permitan implantar el modelo así como un modelo de madurez en 4 niveles.

3.2. Marco de Gestión del Conocimiento Aplicado al Riesgo en TI

El marco de gestión de riesgos de TI en función de la Gestión del Conocimiento se desarrolla tomando como referencia los dominios, procesos y actividades definidos en el marco de gestión de riesgos Risk IT [11], asociando para cada proceso las herramientas, técnicas, factores y actividades de gestión del conocimiento presentados anteriormente en el estado del arte de Gestión del Conocimiento, según corresponda a cada proceso de gestión del riesgo.

Para ello se implementa para cada dominio del modelo de gestión del riesgo Risk IT [11], una matriz de 3 columnas donde en la primer columna se detalla cada uno de los procesos y actividades del dominio, en la segunda columna se presentan los pasos y actividades de gestión del conocimiento a aplicar para mejorar el proceso del riesgo indicado en la primera columna. En la tercer columna se indican los pasos a seguir para la implementación de las actividades de gestión del conocimiento que mejoran el proceso de gestión del riesgo correspondiente.

A continuación se presenta la estructura que tendrá la matriz que se definirá para cada proceso y actividad de cada dominio de Risk IT:

Tabla 1 Vínculo entre procesos/actividades Risk IT y Gestión del Conocimiento

Proceso/Actividad de un Dominio Risk IT (RG, RE,RR)	Gestión del Conocimiento aplicado al Proceso	Implementación de la Gestión del Conocimiento aplicado al Proceso

Luego se define una matriz donde se detallan para cada proceso de gestión del riesgo las etapas, herramientas, técnicas y factores de gestión del conocimiento presentados en el estado del arte de Gestión del Conocimiento, implicados en el proceso de gestión de riesgo correspondiente, según los pasos y actividades identificados en la tabla anterior, para la mejora del proceso e implementación de las actividades de gestión del conocimiento.

A continuación se presenta la estructura que tendrá la matriz que detalla las etapas, herramientas, técnicas y factores para cada proceso/actividad del dominio Risk IT:

Tabla 2 Vínculo entre procesos/actividades de Risk IT y etapas, herramientas, técnicas y factores de Gestión del Conocimiento

Proceso/Actividad de un Dominio Risk IT (RG, RE,RR)	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados

Finalmente, se define para el dominio correspondiente, las matrices RACI de cada proceso del dominio, para la cual en cada actividad del proceso, se identifica el rol de cada función, lo que permite identificar las responsabilidades y su participación en el proceso.

Las funciones definidas son las siguientes: Directivos, Director Ejecutivo (CEO), Jefe de Riesgo (CRO), Jefe de Conocimiento (CKO), Jefe Financiero (CFO), Comité de Riesgos, Dueño de procesos de negocio, Funciones de control de Riesgo, Recursos Humanos y Auditoría y Control. En las PyMEs podrían no estar definidas todas las funciones o ser ejercidas más de una función por la misma persona, por lo que el rol de cada persona, estará dado según el conjunto de las funciones que desempeña.

Los roles definidos son los siguientes: Ninguno (en blanco), Informado, Consultado, Responsable y Responsable que autoriza.

El rol Informado indica que para quienes ejercen esa función, en esa actividad, serán informados sobre la misma.

El rol Consultado, indica que para quienes ejercen esa función, en esa actividad, serán consultados para el desarrollo de la misma.

El rol Responsable, indica que quienes ejercen esa función en esa actividad, son responsables de ella.

El rol Responsable que autoriza, indica que quienes ejercen esta función, en esa actividad, son los responsables de autorizar y llevar adelante dicha actividad. Para cada proceso está definida una única función a cargo de este rol.

A continuación se presenta la estructura que tendrá la matriz RACI que detalla para cada rol su responsabilidad y participación en cada proceso de un dominio de Risk IT:

Tabla 3 Matriz RACI de procesos/actividades de Risk IT de un dominio para cada rol

Funciones	Actividades principales											
	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
Actividad 1	C	A	R	R	R	R	I	C	C	C	C	C
Actividad 2	I	I	A	C	R	C	I	I	C	C		C
Actividad 3	A	C	R	C	C	C	C	C	C	C	C	C
Actividad 4	C	A	R	C	R	R	C	R	R	R	R	C
Actividad 5	A	R	R	R	R	R	R	R	R	R	R	R
Actividad 6	R	R	A	R	R	R	R	R	R	R	R	R

Nota : R – Responsable A – Responsable (autoriza) C – Consultado I - Informado

El [Anexo XIV] presenta la lista completa de las matrices separadas por cada dominio de Risk IT.

3.3. Modelo de Madurez de Gestión del Conocimiento Aplicado al Riesgo en TI

A partir del modelo de madurez de alineamiento estratégico de TI definido en [1] y tomando como base los procesos definidos en el mismo, así como del análisis de la situación de la gestión del conocimiento en PyMEs del Uruguay [2], del estudio empírico realizado sobre estas empresas y los problemas de gobernabilidad de TI que presentan, teniendo en cuenta las recomendaciones indicadas para mitigarlos [Anexo I], así como en base al marco definido en el capítulo anterior de este documento, es que se crea un modelo de gestión del riesgo basado en la gestión del conocimiento para este tipo de empresas en Uruguay.

Se analiza la incidencia de la gestión del conocimiento en el Gobierno de TI, y más precisamente en la gestión de riesgos, incorporando el uso de las herramientas, técnicas y factores de la gestión del conocimiento que se determinaron en el marco que se definió en el punto anterior de este documento.

Se define así una escala ascendente de niveles de madurez respecto a la gestión del conocimiento aplicada a la gestión del riesgo, donde se cuenta con 4 niveles de madurez, siguiendo el planteo presentado en [1]. Cada nivel representa el estado de los procesos de gestión del conocimiento que presenta una empresa PyME en dicho nivel. Cada nivel del modelo contiene implícitamente a sus niveles anteriores.

Cuenta así con un nivel inicial básico, donde no existe una conciencia sobre la gestión del conocimiento asociada a la gestión del riesgo o existe pero es limitada o se limita a procesos ad hoc. El nivel siguiente, donde el conocimiento es gestionado y está establecido como un elemento a tener en cuenta para la gestión del riesgo en TI y su efecto sobre el negocio. Un tercer nivel que se presenta como predecible, donde los procesos están definidos y existe una sistematización de los procedimientos de gestión del conocimiento que son planificados.

Finalmente existe un cuarto y último nivel avanzado, donde se cuenta con los procesos de gestión del conocimiento que son integrados totalmente y mejorados continuamente por medio de procesos de mejora continua.

El [Anexo XV] detalla para cada nivel, como aplica la gestión del conocimiento, discriminado por los aspectos Estrategia de TI, Portfolio Estratégico, Proyectos y Operaciones, respecto a los ítems, proyección de futuro, orientación al usuario, contribución al negocio y excelencia operativa definidos en [1].

4. Indicadores

Se desarrollan indicadores para poder implementar el marco de gestión del conocimiento basado en la gestión del riesgo así como el modelo de madurez en empresas de tipo PyMEs. Se definen los indicadores detallados en el [Anexo XVI], con los que se determina un valor asociado al proceso en el cual aplica. Luego se presentan en el mismo anexo un mapa de indicadores, que permite visualizar las relaciones de cada indicador con los procesos y dominios del Risk IT al cual aplican, de forma gráfica.

Los indicadores se dividen en 2 categorías Básica y Avanzada, brindando así la posibilidad de evaluar empresas que no cuenten con una estructura u organización que les permita implementar todos los indicadores, pudiendo comenzar con los indicadores básicos y luego pasar a implementar los indicadores avanzados a medida que se cuente con información para su medida.

Se definen los indicadores para cada dominio del marco creado y dentro de ellos para cada proceso y actividad.

4.1. Ponderación de indicadores según el nivel de madurez

Para cada nivel de madurez del modelo de gestión del riesgo basado en la gestión del conocimiento, se establecen a los indicadores, las medidas asociadas.

En caso de no existir o de no poder definirse una medida para el indicador, se asigna el valor No aplica para ese indicador en el nivel de madurez. Esto permitirá establecer en qué nivel de madurez de Gestión del Riego basado en Gestión del Conocimiento se encuentra la empresa para cada indicador, permitiendo así, visualizar el estado de la empresa con una visión general de la misma, facilitando la determinación y priorización de las acciones a tomar para superar el nivel de madurez y pasar al siguiente nivel del modelo.

El [Anexo XVII] presenta para cada nivel de madurez (de 1 a 4), el detalle en cada proceso / indicador de la medida que aplica para dicho indicador en el nivel de madurez correspondiente.

Luego, se detalla para cada indicador, la referencia bibliográfica y argumentación teórica que justifica su definición y uso, * como métrica para el modelo.

5. Experimentación

La experimentación se desarrolla aplicando el modelo de gestión del riesgo basado en la gestión del conocimiento, en dos empresas de tipo PyMEs de Uruguay, para las cuales se evalúa su situación según este modelo, haciendo uso de la planilla de indicadores por proceso presentada en el Anexo VII, definida para tal fin. De esta forma se determina el nivel al cual pertenece la empresa evaluada y cuál o cuáles serán los procesos a mejorar para pasar al siguiente nivel de madurez en el modelo.

Se divide el trabajo de experimentación en 3 etapas, una inicial de planificación de la experimentación donde se presentan las empresas y la forma en que se desarrolla el relevamiento de la información necesaria para la valoración a realizar sobre la empresa. Luego se presenta la etapa de ejecución, en la cual se detalla los datos relevados de cada empresa y las planillas resultado del relevamiento. Finalmente se presenta la etapa de conclusión y evaluación de los datos relevados y del proceso de experimentación.

5.1. Planificación

A partir de los indicadores presentados, se realiza la experimentación del marco y modelo de gestión del conocimiento basado en la gestión del riesgo.

Se aplica sobre dos empresas de tipo PyMEs de Uruguay, una del rubro informático y otra del ámbito inmobiliario. Ambas empresas cuentan con menos de 19 empleados, perteneciendo al rango de pequeñas empresas [Anexo II].

La empresa del rubro informático brinda servicios de desarrollo de software y aplicaciones a medida para empresas y particulares, hardware, redes, telecomunicaciones, servicio técnico especializado, diseño gráfico y web, educación y capacitación informática especializada para toda edad, cursos de administración, ventas y marketing, venta de equipos e insumos. También cuenta con una sucursal que opera como centro de fotocopiado e impresión digital, servicio de papelería y encuadernación, espacio de cibercafé y entretenimientos, con atención personalizada y especializada a clientes.

Dada la diversidad de servicios que provee la empresa, existen distintas áreas de trabajo como ser: desarrollo de software, servicio técnico y redes, capacitación, formación, entretenimiento y centro de fotocopiado e impresión digital.

Para el relevamiento de la información se encuesta al director de la empresa, quien cuenta con el conocimiento global de la misma, tanto a nivel del negocio como de los aspectos técnicos relevantes para su funcionamiento (perfil propio de empresas de este tipo) lo cual permite una mayor precisión del relevamiento a realizar.

Respecto a la empresa inmobiliaria, esta es una pequeña empresa, con un director y un responsable que comparten las actividades de gestión de la empresa. Para su relevamiento se encuesta al responsable de la misma. La inmobiliaria desarrolla tareas de alquiler y venta de apartamentos y casas, así como también la administración de las mismas. Además de los contratos de alquiler y venta, se realizan las publicaciones de los inmuebles en variados sitios, así como en el sitio de la empresa.

Cuenta con un sistema de gestión desarrollado a medida, que se encarga de la facturación y gestión de clientes. La empresa no realiza las tareas de control de la red, soporte a equipos, comunicaciones, así como la gestión del sistema que utilizan, todas estas actividades referentes al ámbito informático son tercerizadas a distintas empresas encargadas de su mantenimiento y desarrollo. Se presentó hace algún tiempo un evento en el cual se generó una ruptura del disco donde se contaba con la información de gestión, razón por la cual se procedió a realizar respaldos en discos extraíbles, para mitigar el riesgo de una posible pérdida como la ocurrida, lo cual alertó a la empresa sobre el riesgo existente al no contar con respaldos.

Para el relevamiento se utilizará la planilla de experimentación elaborada para este fin (Figura 15), que se basa en la planilla presentada en el Anexo VII. En las columnas de Valoración el encuestador ingresa el valor determinado para el proceso e indicador correspondiente, cuyo valor pertenece al rango de valores posibles, que se presentan en el Anexo VII para los distintos niveles del modelo de madurez. Con el fin de facilitar la comparación del resultado obtenido para ambas empresas, se cuenta con una columna de valoración para cada empresa, con el color indicativo del nivel asociado correspondiente a la valoración para ese proceso e indicador.

Durante la encuesta se contará con la planilla a completar así como la planilla de referencia presentada en el Anexo VII, lo cual facilita el desarrollo de la misma.

De esta forma, al finalizar la encuesta se contará con un detalle de los niveles asociados a cada proceso/indicador, que se pueden consultar rápidamente, así como los ítems a mejorar para llegar al nivel siguiente del modelo de madurez.

Figura 15 Planilla de Experimentación

	Proceso	Indicador	Valoración
RG	Proceso Gobierno del Riesgo		
RG 1.1	Desarrollar en una empresa el marco específico de gestión de riesgos de TI	1. Porcentaje de variables de negocio para las cuales se ha identificado y registrado los puntos de TI que pueden aportar valor al negocio, para los cuales existe un análisis de tolerancia al riesgo. Registro de variables con tolerancia al riesgo en los rangos: 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100% 2. Existencia de mapas de conocimiento que vinculan los eventos de TI identificados.	
RG 1.2	Proponer los umbrales de tolerancia de riesgos de TI	1. Porcentaje de procesos de negocio que cuentan con medidas de riesgo y niveles de tolerancia asociados. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	
		2. Existencia de recursos humanos capacitados para la definición de umbrales de tolerancia de riesgos de TI. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	

	Proceso	Indicador	Valoración
RG 1.3	Aprobar la tolerancia al riesgo	1. Existencia de mapas de conocimiento y base de conocimiento de todas las áreas de la empresa con umbrales de riesgo por área de negocio.	
RG 1.4	Alinear la política de riesgos de TI	1. Existencia de base de conocimiento de la organización con apetito al riesgo y tolerancia de cada área de negocio.	
		2. Nro de horas de reunión de grupos de expertos por cada área sobre el número de áreas de negocio de la empresa, dedicados a la definición del apetito y tolerancia al riesgo de cada área respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
RG 1.5	Promover los riesgos de TI – cultura consciente	1. Horas dedicadas en cursos sobre nro de personas capacitadas en gestión del riesgo para cada área de negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		2. Existencia de base de conocimientos con registro de acciones y buenas prácticas en gestión del riesgo de cada área de negocio.	
		3. Existencia del rol CKO dedicado a la comunicación de la política de gestión del riesgo en la organización. 4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	
RG 1.6	Promover una comunicación efectiva de los riesgos de TI	1. Existencia de un plan de comunicación de riesgos 2. Existencia de una base de conocimiento organizacional accesible por responsables y directores con información sobre amenazas e impacto de riesgos por área.	
		3. Nro de amenazas por área de negocio registradas en la base de conocimiento. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100% 4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	

	Proceso	Indicador	Valoración
RG 2.1	Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes.	
		2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	
RG 2.2	Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial	1. Horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		2. Horas de reuniones dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	
RG 2.3	Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa	1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.	
		2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa. 3. Porcentaje de recursos de la empresa capacitados o que asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	
RG 2.4	Proporcionar recursos adecuados para la gestión de riesgos	1. Nro de horas en capacitación al personal de cada área en gestión del riesgo, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	

	Proceso	Indicador	Valoración
		2. Existencia de una base de conocimiento de la organización y mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.	
RG 2.5	Garantizar el aseguramiento independiente sobre la gestión de riesgos	1. Existe una base de conocimiento con el registro del apetito al riesgo y tolerancia que permite la gestión del riesgo por parte del director de TI y director general.	
		2. Existencia de mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.	
		3. Horas en capacitación de recursos humanos asegurando su independencia en la gestión de riesgos respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
RG 3.1	Ganancia de la gestión de compra para el enfoque de análisis de riesgos	1. Existe una base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo.	
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	
		3. Horas de capacitación o reuniones que permitan interpretar los informes de análisis de riesgo y brechas existentes con el riesgo empresarial, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		4. Horas de capacitación en concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos de la empresa, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
RG 3.2	Aprobar el análisis de riesgos de TI	1. Existe una base de conocimiento única para las distintas áreas de la empresa accesible a todos los directores de área que permite registrar, transmitir y usar dicho conocimiento. 2. Nro de horas en capacitación y reuniones para la formación de los directores de área en la cultura de gestión del riesgo a través de la gestión del conocimiento respecto al total de horas de los directores. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	

	Proceso	Indicador	Valoración
RG 3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.</p> <p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	
		<p>3. Horas de capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RG 3.4	Aceptar los riesgos de TI	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.</p> <p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	
		<p>3. Horas de capacitación en formación al personal sobre aceptación y gestión del riesgo de TI para el negocio de cada área de la empresa respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RG 3.5	Priorizar actividades de respuesta de riesgos de TI	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa disponible para el director general y director de TI, que permita registrar métricas para el seguimiento del cumplimiento de las actividades de TI, así como priorización de las mismas, con información sobre el apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles.</p> <p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p> <p>3. Horas de capacitación y formación al director general y de TI sobre seguimiento y planificación de riesgos en TI respecto al total de horas de los directores general y de TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	

	Proceso	Indicador	Valoración
RE	Gestión del Riesgo Proceso Evaluación del Riesgo (RE)		
RE 1.1	Establecer y mantener un modelo para la recolección de datos	1. Existe apoyo explícito de la dirección para la concreción de la recopilación de datos para la formación de un repositorio único de conocimiento, así como en la culturización en gestión del conocimiento en la empresa.	
		2. Existe una estrategia de adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	
		3. Existe una implementación para la adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	
		4. Horas de capacitación y formación realizadas con el personal de la empresa respecto a la recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento en la organización, respecto al total de horas del personal. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
RE 1.2	Recopilar datos sobre el entorno externo	1. Horas de reuniones de benchmarking, charlas informales y con expertos, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
RE 1.3	Recopilar datos sobre eventos de riesgo	1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
RE 1.4	Identificar factores de riesgo	1. Horas de reuniones de charlas con expertos, coaching, comunidades de práctica realizadas por directivos de TI y de las restantes áreas de la empresa, aplicadas para la identificación de riesgos, asociados a proyectos, programas, servicios existentes y futuros, etc. que pueden generar eventos de riesgo, respecto al total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	

	Proceso	Indicador	Valoración
RE 2.1	Definir Alcance del Análisis de Riesgo	<p>2. Existencia de una base de conocimiento organizacional donde se integra información sobre proyectos, programas, servicios e incidentes.</p> <p>1. Horas de capacitación y formación al personal responsable de la gestión del riesgo y del negocio de la empresa, en cuanto a gestión y evaluación del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
		<p>2. Horas de reuniones de charlas con expertos, benchmarking, realizadas con el personal responsable de la gestión del riesgo y el negocio sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RE 2.2	Estimación de riesgos en TI	<p>1. Horas de capacitación y formación a los responsables del riesgo y de negocio de la empresa, sobre análisis de información de riesgo (factores, frecuencia, magnitud y tolerancia al riesgo) para la estimación y definición de controles respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
		<p>2. Existencia de un CMS disponible para el análisis en la estimación de riesgos.</p>	
		<p>3. Horas de reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
		<p>4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos en el CMS de la empresa.</p>	
RE 2.3	Identificar las opciones de respuesta de riesgo	<p>1. Horas de capacitación y formación a los directivos y responsables del riesgo sobre identificación de respuestas de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de un CMS disponible para la consulta y actualización de respuestas de riesgo.</p>	

	Proceso	Indicador	Valoración
		<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas de riesgos en el CMS de la empresa.</p>	
RE 2.4	Realizar una revisión por pares de los resultados de análisis de riesgos de TI	<p>1. Horas de capacitación y formación a los responsables del riesgo sobre la aplicación de técnicas para el análisis de riesgos de TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RE 3.1	Mapa de recursos de TI para procesos de negocio	<p>2. Existencia de un CMS disponible para la actualización de la información sobre riesgos de TI en la empresa.</p> <p>3. Horas de reuniones de charlas con expertos, charlas formales e informales, coaching en asignación de recursos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>4. Aplicación de sistemas expertos en la resolución de la asignación de recursos.</p> <p>1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.</p>	
		<p>2. Horas de capacitación y formación a los responsables del riesgo en la empresa, sobre uso y análisis de mapas de conocimiento respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RE 3.2	Determinar la criticidad de negocios de los recursos de TI	<p>1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.</p>	
		<p>2. Horas de capacitación y formación a los responsables de la gestión de los recursos en las distintas áreas de la empresa, sobre la determinación de criticidad de los recursos según los requerimientos de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	

	Proceso	Indicador	Valoración
RE 3.3	Entender las capacidades de TI	<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales para la definición de la criticidad de los recursos de TI en cada área respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>4. Existencia de un CMS con información sobre riesgos, recursos y su criticidad.</p> <p>1. Horas de capacitación y formación de los responsables de TI y responsables de cada área, para la evaluación de las capacidades disponibles y análisis de situación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
		2. Existe plan de capacitación de los responsables de cada área y de TI, sobre gestión del riesgo de TI.	
		<p>3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.</p> <p>4. Existencia de un CMS con información sobre las capacidades y requerimientos en TI de la empresa.</p>	
		<p>5. Horas de reuniones de charlas formales e informales, consultas a expertos, sobre análisis de las capacidades existentes en TI y sus requerimientos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RE 3.4	Actualización de los componentes del escenario de riesgos de TI	<p>1. Horas de capacitación y formación de los responsables de negocio, riesgo y TI, para la evaluación de escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
		2. Existencia de un CMS con información sobre riesgos y distintos escenarios de riesgo.	
		3. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre análisis de distintos escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	

	Proceso	Indicador	Valoración
RE 3.5	Mantener los riesgos de TI y mapa de registro de riesgos de TI	1. Horas de capacitación y formación de los responsables de negocio y TI, para la actualización de riesgos de TI y definición de perfil de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		2. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre definición de perfil de riesgo de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
RE 3.6	Diseñar y comunicar los indicadores de riesgo de TI	3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes. 1. Existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo en TI en la empresa.	
		2. Horas de reuniones de charlas formales y consultas a expertos sobre difusión de indicadores de riesgo de la empresa respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		3. Existencia de conocimiento actualizado sobre buenas prácticas en difusión de indicadores en la base de conocimiento de la empresa.	
RR	Gestión del Riesgo Proceso Respuesta del Riesgo (RR)		
RR 1.1	Informe de los resultados de análisis de riesgos de TI	1. Horas de reuniones de charlas formales, consultas a expertos, coaching, mentoring sobre gestión de la comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		2. Horas de capacitación y formación sobre técnicas y herramientas de comunicación y coordinación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		3. Existe un CMS a nivel de la organización que permite adquirir el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, por parte de los responsables de negocio, riesgo y directores.	

	Proceso	Indicador	Valoración
RR 1.2	Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	1. Horas de reuniones de charlas formales e informales, consultas a expertos, coaching, mentoring sobre generación de informes y comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		2. Existe un CMS a nivel de la organización que permite la distribución de la información estratégica resultado de la gestión de riesgos.	
		3. Existencia de conocimiento actualizado en el CMS sobre lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados.	
RR 1.3	Interpretar resultados de la evaluación independiente de TI	1. Existencia de conocimiento actualizado en el CMS para el análisis de acciones correctivas e identificación de oportunidades de mejora.	
		2. Horas de capacitación y formación de recursos humanos de la empresa en el análisis del conocimiento del CMS para la generación de planes de acción correctiva respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		3. Existencia de un plan de acción correctiva	
RR 1.4	Identificar TI – Oportunidades relacionadas	4. Horas de reuniones de charlas formales e informales, contacto personal, mentoring sobre el análisis de acciones correctivas y mejoras en la gestión del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		1. Horas de capacitación y formación de recursos humanos responsables de TI y del negocio de la empresa en el análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		2. Horas de reuniones de charlas con expertos, coaching, benchmarking sobre optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
RR 2.1	Controles del inventario	1. Existencia de conocimiento actualizado en el CMS para el control de inventario de riesgos.	

	Proceso	Indicador	Valoración
		<p>2. Horas de capacitación y formación de recursos humanos de la empresa en el control de inventarios de riesgo y clasificación de controles respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Horas de reuniones de charlas formales e informales, coaching y mentoring sobre control del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RR 2.2	Supervisar la alineación operacional de los umbrales de tolerancia al riesgo	1. Existe apoyo explícito de la dirección en la definición de indicadores de riesgo y definición de umbrales de tolerancia al riesgo.	
		2. Existe un CMS de la organización con riesgos, tolerancia al riesgo y umbrales, disponible para la supervisión de la alineación operacional de los umbrales a la tolerancia al riesgo.	
		<p>3. Existen reuniones de charlas y grupos de expertos para el logro de la aceptación de indicadores por parte de las áreas operativas y dirección.</p> <p>4. Horas de capacitación a la dirección en la definición de umbrales de tolerancia al riesgo y supervisión respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RR 2.3	Responder a la exposición al riesgo descubierto y la oportunidad	1. Existencia de conocimiento actualizado en el CMS para la respuesta al riesgo.	
		2. Horas de reuniones de charlas formales e informales, coaching, mentoring sobre respuestas al riesgo descubierto y oportunidades respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		3. Existencia de un mapa de conocimiento que facilite el acceso y distribución de los riesgos descubiertos y oportunidades.	
RR 2.4	Implementar los controles	1. Existe un CMS actualizado con el conocimiento sobre controles de riesgo.	

	Proceso	Indicador	Valoración
		<p>2. Horas de reuniones de coaching, mentoring, charlas formales e informales, sobre implementación de controles respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existencia de un mapa de conocimientos actualizado que cuenta con la distribución del riesgo y controles existentes en la organización.</p>	
		<p>4. Horas de capacitación y formación en la implementación de controles y uso de mapas de conocimiento para el mismo respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RR 2.5	Informe del progreso del plan de acción de riesgos de TI	<p>1. Horas de capacitación al personal de TI y responsables del riesgo, en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de reuniones de charlas, grupos de expertos, benchmarking en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
		<p>3. Horas de reuniones destinadas a la comunicación sobre el progreso del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RR 3.1	Mantener los planes de respuesta a incidentes	<p>1. Existe un CMS actualizado de respuestas a incidentes, accesible a los responsables de TI y gestión del riesgo.</p>	
		<p>2. Horas de reuniones en charlas, grupos de expertos sobre comunicación y gestión de planes de respuesta respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
RR 3.2	Supervisión de riesgos de TI	<p>1. Horas de capacitación a responsables del riesgo y auditores sobre supervisión de riesgo de TI respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	
		<p>2. Existencia de un CMS sobre riesgos y límites de la organización accesible a los responsables del riesgo y auditores.</p>	

	Proceso	Indicador	Valoración
		3. Horas de reuniones con grupos de expertos, charlas formales e informales sobre mejora en los riesgos de TI en base a los riesgos y límites tolerados respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
RR 3.3	Iniciar planes de respuesta a incidentes	1. Horas de capacitación y formación de responsables de la gestión y el riesgo de la empresa, en el logro de las mejores respuestas de cada incidente y el uso del CMS de la organización para ello respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20% 2. Horas de reuniones en charlas formales e informales y benchmarking para lograr las mejores respuestas a incidentes y correcta distribución del conocimiento a los interesados respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		3. Existencia de una base de conocimiento actualizada con categorías de hechos y respuestas.	
RR 3.4	Comunicar las lecciones aprendidas de eventos de riesgo	1. Horas de capacitación y formación de responsables de TI y del riesgo de la empresa, en la identificación de las causas de problemas respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		2. Horas de capacitación en charlas, grupos de expertos y benchmarking sobre identificación de causas de problemas respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	
		3. Existencia de un CMS actualizado con datos históricos y recientes de acontecimientos adversos y pérdidas.	

5.2. Ejecución

Luego de realizadas las encuestas según lo planificado, se obtienen las planillas de resultado que se presentan a continuación:

Figura 16 Planilla resultado de las encuestas

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
RG	Proceso Gobierno del Riesgo			
RG 1.1	Desarrollar en una empresa el marco específico de gestión de riesgos de TI	<p>1. Porcentaje de variables de negocio para las cuales se ha identificado y registrado los puntos de TI que pueden aportar valor al negocio, para los cuales existe un análisis de tolerancia al riesgo.</p> <p>Registro de variables con tolerancia al riesgo en los rangos: 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	20-40%	0-20%
		2. Existencia de mapas de conocimiento que vinculan los eventos de TI identificados.	No Existe	No Existe
RG 1.2	Proponer los umbrales de tolerancia de riesgos de TI	<p>1. Porcentaje de procesos de negocio que cuentan con medidas de riesgo y niveles de tolerancia asociados. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p> <p>2. Existencia de recursos humanos capacitados para la definición de umbrales de tolerancia de riesgos de TI. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	0-20%	0-20%
RG 1.3	Aprobar la tolerancia al riesgo	1. Existencia de mapas de conocimiento y base de conocimiento de todas las áreas de la empresa con umbrales de riesgo por área de negocio.	No Existe	No Existe
RG 1.4	Alinear la política de riesgos de TI	1. Existencia de base de conocimiento de la organización con apetito al riesgo y tolerancia de cada área de negocio.	No Existe	No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
		<p>2. Nro de horas de reunión de grupos de expertos por cada área sobre el número de áreas de negocio de la empresa, dedicados a la definición del apetito y tolerancia al riesgo de cada área respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%
RG 1.5	Promover los riesgos de TI – cultura consciente	<p>1. Horas dedicadas en cursos sobre nro de personas capacitadas en gestión del riesgo para cada área de negocio respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%
		<p>2. Existencia de base de conocimientos con registro de acciones y buenas prácticas en gestión del riesgo de cada área de negocio.</p>	Existe	No Existe
		<p>3. Existencia del rol CKO dedicado a la comunicación de la política de gestión del riesgo en la organización.</p>	No Aplica	No Aplica
		<p>4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.</p>	No Existe	No Existe
RG 1.6	Promover una comunicación efectiva de los riesgos de TI	<p>1. Existencia de un plan de comunicación de riesgos</p>	No Aplica	No Aplica
		<p>2. Existencia de una base de conocimiento organizacional accesible por responsables y directores con información sobre amenazas e impacto de riesgos por área.</p>	Existe	No Existe
		<p>3. Nro de amenazas por área de negocio registradas en la base de conocimiento.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	0-20%	0-20%
		<p>4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.</p>	Existe	No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
RG 2.1	Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	<p>1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes.</p> <p>2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	No Aplica	No Aplica
RG 2.2	Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial	<p>1. Horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%
		<p>2. Horas de reuniones dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	0-5%	0-5%
RG 2.3	Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa	<p>1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.</p>	Existe	No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
		2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.	Existe	No Existe
		3. Porcentaje de recursos de la empresa capacitados o que asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	0-20%	0-20%
RG 2.4	Proporcionar recursos adecuados para la gestión de riesgos	1. Nro de horas en capacitación al personal de cada área en gestión del riesgo, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
RG 2.5	Garantizar el aseguramiento independiente sobre la gestión de riesgos	2. Existencia de una base de conocimiento de la organización y mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable. 1. Existe una base de conocimiento con el registro del apetito al riesgo y tolerancia que permite la gestión del riesgo por parte del director de TI y director general.	Existe No Existe	No Existe No Existe
RG 3.1	Ganancia de la gestión de compra para el enfoque de análisis de riesgos	2. Existencia de mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable. 3. Horas en capacitación de recursos humanos asegurando su independencia en la gestión de riesgos respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20% 1. Existe una base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo.	Existe 0-5% No Existe	No Existe 0-5% No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	No Existe	No Existe
		3. Horas de capacitación o reuniones que permitan interpretar los informes de análisis de riesgo y brechas existentes con el riesgo empresarial, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		4. Horas de capacitación en concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos de la empresa, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	5-10%	0-5%
RG 3.2	Aprobar el análisis de riesgos de TI	1. Existe una base de conocimiento única para las distintas áreas de la empresa accesible a todos los directores de área que permite registrar, transmitir y usar dicho conocimiento.	Existe	No Existe
		2. Nro de horas en capacitación y reuniones para la formación de los directores de área en la cultura de gestión del riesgo a través de la gestión del conocimiento respecto al total de horas de los directores. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Existe	No Existe
RG 3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa. 2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Existe No Existe	No Existe No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
RG 3.4	Aceptar los riesgos de TI	3. Horas de capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	5-10%	0-5%
		1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.	Existe	No Existe
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	No Existe	No Existe
		3. Horas de capacitación en formación al personal sobre aceptación y gestión del riesgo de TI para el negocio de cada área de la empresa respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
RG 3.5	Priorizar actividades de respuesta de riesgos de TI	1. Existe una base de conocimiento para la gestión del riesgo en la empresa disponible para el director general y director de TI, que permita registrar métricas para el seguimiento del cumplimiento de las actividades de TI, así como priorización de las mismas, con información sobre el apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles.	Existe	No Existe
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Existe	No Existe
		3. Horas de capacitación y formación al director general y de TI sobre seguimiento y planificación de riesgos en TI respecto al total de horas de los directores general y de TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	5-10%	0-5%

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
RE	Gestión del Riesgo Proceso Evaluación del Riesgo			
RE 1.1	Establecer y mantener un modelo para la recolección de datos	<p>1. Existe apoyo explícito de la dirección para la concreción de la recopilación de datos para la formación de un repositorio único de conocimiento, así como en la culturización en gestión del conocimiento en la empresa.</p> <p>2. Existe una estrategia de adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.</p>	Existe	No Existe
		3. Existe una implementación para la adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	No Existe	No Existe
RE 1.2	Recopilar datos sobre el entorno externo	<p>4. Horas de capacitación y formación realizadas con el personal de la empresa respecto a la recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento en la organización, respecto al total de horas del personal.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>1. Horas de reuniones de benchmarking, charlas informales y con expertos, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%
RE 1.3	Recopilar datos sobre eventos de riesgo	<p>1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	5-10%	0-5%

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
RE 1.4	Identificar factores de riesgo	<p>1. Horas de reuniones de charlas con expertos, coaching, comunidades de práctica realizadas por directivos de TI y de las restantes áreas de la empresa, aplicadas para la identificación de riesgos, asociados a proyectos, programas, servicios existentes y futuros, etc. que pueden generar eventos de riesgo, respecto al total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	5-10%	0-5%
RE 2.1	Definir Alcance del Análisis de Riesgo	<p>2. Existencia de una base de conocimiento organizacional donde se integra información sobre proyectos, programas, servicios e incidentes.</p> <p>1. Horas de capacitación y formación al personal responsable de la gestión del riesgo y del negocio de la empresa, en cuanto a gestión y evaluación del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de reuniones de charlas con expertos, benchmarking, realizadas con el personal responsable de la gestión del riesgo y el negocio sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Existe y Desarrolla</p> <p>0-5%</p> <p>0-5%</p>	<p>No Existe</p> <p>0-5%</p> <p>0-5%</p>
RE 2.2	Estimación de riesgos en TI	<p>1. Horas de capacitación y formación a los responsables del riesgo y de negocio de la empresa, sobre análisis de información de riesgo (factores, frecuencia, magnitud y tolerancia al riesgo) para la estimación y definición de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	5-10%	0-5%
		<p>2. Existencia de un CMS disponible para el análisis en la estimación de riesgos.</p>	No Existe	No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
		<p>3. Horas de reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%
RE 2.3	Identificar las opciones de respuesta de riesgo	<p>4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos en el CMS de la empresa.</p> <p>1. Horas de capacitación y formación a los directivos y responsables del riesgo sobre identificación de respuestas de riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de un CMS disponible para la consulta y actualización de respuestas de riesgo.</p> <p>3. Horas de reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas de riesgos en el CMS de la empresa.</p>	Existe	No Existe
			0-5%	0-5%
			Existe	No Existe
			0-5%	0-5%
RE 2.4	Realizar una revisión por pares de los resultados de análisis de riesgos de TI	<p>1. Horas de capacitación y formación a los responsables del riesgo sobre la aplicación de técnicas para el análisis de riesgos de TI respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
		2. Existencia de un CMS disponible para la actualización de la información sobre riesgos de TI en la empresa.	Existe	No Existe
		3. Horas de reuniones de charlas con expertos, charlas formales e informales, coaching en asignación de recursos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		4. Aplicación de sistemas expertos en la resolución de la asignación de recursos.	Ocasional	
RE 3.1	Mapa de recursos de TI para procesos de negocio	1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.	Existe	No Existe
		2. Horas de capacitación y formación a los responsables del riesgo en la empresa, sobre uso y análisis de mapas de conocimiento respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
RE 3.2	Determinar la criticidad de negocios de los recursos de TI	1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.	Existe	No Existe
		2. Horas de capacitación y formación a los responsables de la gestión de los recursos en las distintas áreas de la empresa, sobre la determinación de criticidad de los recursos según los requerimientos de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		3. Horas de reuniones de charlas con expertos, charlas formales e informales para la definición de la criticidad de los recursos de TI en cada área respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
RE 3.3	Entender las capacidades de TI	4. Existencia de un CMS con información sobre riesgos, recursos y su criticidad.	No Existe	No Existe
		1. Horas de capacitación y formación de los responsables de TI y responsables de cada área, para la evaluación de las capacidades disponibles y análisis de situación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	5-10%	0-5%
		2. Existe plan de capacitación de los responsables de cada área y de TI, sobre gestión del riesgo de TI.	Existe	No Existe
		3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.	Existe	No Existe
RE 3.4	Actualización de los componentes del escenario de riesgos de TI	4. Existencia de un CMS con información actualizada sobre las capacidades y requerimientos en TI de la empresa.	Existe	No Existe
		5. Horas de reuniones de charlas formales e informales, consultas a expertos, sobre análisis de las capacidades existentes en TI y sus requerimientos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	5-10%	0-5%
		1. Horas de capacitación y formación de los responsables de negocio, riesgo y TI, para la evaluación de escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		2. Existencia de un CMS con información sobre riesgos y distintos escenarios de riesgo.	No Existe	No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
		3. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre análisis de distintos escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
RE 3.5	Mantener los riesgos de TI y mapa de registro de riesgos de TI	1. Horas de capacitación y formación de los responsables de negocio y TI, para la actualización de riesgos de TI y definición de perfil de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		2. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre definición de perfil de riesgo de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.	Existe	No Existe
RE 3.6	Diseñar y comunicar los indicadores de riesgo de TI	1. Existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo en TI en la empresa. 2. Horas de reuniones de charlas formales y consultas a expertos sobre difusión de indicadores de riesgo de la empresa respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe 5-10%	No Existe 0-5%
		3. Existencia de conocimiento actualizado sobre buenas prácticas en difusión de indicadores en la base de conocimiento de la empresa.	Existe	No Existe
RR	Gestión del Riesgo Proceso Respuesta del Riesgo (RR)			

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
RR 1.1	Informe de los resultados de análisis de riesgos de TI	<p>1. Horas de reuniones de charlas formales, consultas a expertos, coaching, mentoring sobre gestión de la comunicación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de capacitación y formación sobre técnicas y herramientas de comunicación y coordinación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%
RR 1.2	Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	<p>3. Existe un CMS a nivel de la organización que permite adquirir el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, por parte de los responsables de negocio, riesgo y directores.</p> <p>1. Horas de reuniones de charlas formales e informales, consultas a expertos, coaching, mentoring sobre generación de informes y comunicación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	No Existe	No Existe
RR 1.3	Interpretar resultados de la evaluación independiente de TI	<p>2. Existe un CMS a nivel de la organización que permite la distribución de la información estratégica resultado de la gestión de riesgos.</p> <p>3. Existencia de conocimiento actualizado en el CMS sobre lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados.</p> <p>1. Existencia de conocimiento actualizado en el CMS para el análisis de acciones correctivas e identificación de oportunidades de mejora.</p>	Existe	No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
		<p>2. Horas de capacitación y formación de recursos humanos de la empresa en el análisis del conocimiento del CMS para la generación de planes de acción correctiva respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existencia de un plan de acción correctiva</p>	0-5%	0-5%
		<p>4. Horas de reuniones de charlas formales e informales, contacto personal, mentoring sobre el análisis de acciones correctivas y mejoras en la gestión del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%
RR 1.4	Identificar TI – Oportunidades relacionadas	<p>1. Horas de capacitación y formación de recursos humanos responsables de TI y del negocio de la empresa en el análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	5-10%	0-5%
		<p>2. Horas de reuniones de charlas con expertos, coaching, benchmarking sobre optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	5-10%	0-5%
RR 2.1	Controles del inventario	<p>1. Existencia de conocimiento actualizado en el CMS para el control de inventario de riesgos.</p>	Existe	No Existe
		<p>2. Horas de capacitación y formación de recursos humanos de la empresa en el control de inventarios de riesgo y clasificación de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
		3. Horas de reuniones de charlas formales e informales, coaching y mentoring sobre control del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
RR 2.2	Supervisar la alineación operacional de los umbrales de tolerancia al riesgo	1. Existe apoyo explícito de la dirección en la definición de indicadores de riesgo y definición de umbrales de tolerancia al riesgo.	No Existe	No Existe
		2. Existe un CMS de la organización con riesgos, tolerancia al riesgo y umbrales, disponible para la supervisión de la alineación operacional de los umbrales a la tolerancia al riesgo.	No Existe	No Existe
		3. Existen reuniones de charlas y grupos de expertos para el logro de la aceptación de indicadores por parte de las áreas operativas y dirección.	Existe	No Existe
		4. Horas de capacitación a la dirección en la definición de umbrales de tolerancia al riesgo y supervisión respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	5-10%	0-5%
RR 2.3	Responder a la exposición al riesgo descubierto y la oportunidad	1. Existencia de conocimiento actualizado en el CMS para la respuesta al riesgo.	Existe	No Existe
		2. Horas de reuniones de charlas formales e informales, coaching, mentoring sobre respuestas al riesgo descubierto y oportunidades respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		3. Existencia de un mapa de conocimiento que facilite el acceso y distribución de los riesgos descubiertos y oportunidades.	Existe	No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
RR 2.4	Implementar los controles	<p>1. Existe un CMS actualizado con el conocimiento sobre controles de riesgo.</p> <p>2. Horas de reuniones de coaching, mentoring, charlas formales e informales, sobre implementación de controles respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	Existe	No Existe
		<p>3. Existencia de un mapa de conocimientos actualizado que cuenta con la distribución del riesgo y controles existentes en la organización.</p>	No Existe	No Existe
RR 2.5	Informe del progreso del plan de acción de riesgos de TI	<p>4. Horas de capacitación y formación en la implementación de controles y uso de mapas de conocimiento para el mismo respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>1. Horas de capacitación al personal de TI y responsables del riesgo, en supervisión del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	5-10%	0-5%
		<p>2. Horas de reuniones de charlas, grupos de expertos, benchmarking en supervisión del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	0-5%
RR 3.1	Mantener los planes de respuesta a incidentes	<p>3. Horas de reuniones destinadas a la comunicación sobre el progreso del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>1. Existe un CMS actualizado de respuestas a incidentes, accesible a los responsables de TI y gestión del riesgo.</p>	Existe	No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
		2. Horas de reuniones en charlas, grupos de expertos sobre comunicación y gestión de planes de respuesta respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
RR 3.2	Supervisión de riesgos de TI	1. Horas de capacitación a responsables del riesgo y auditores sobre supervisión de riesgo de TI respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		2. Existencia de un CMS sobre riesgos y límites de la organización accesible a los responsables del riesgo y auditores.	Existe	No Existe
		3. Horas de reuniones con grupos de expertos, charlas formales e informales sobre mejora en los riesgos de TI en base a los riesgos y límites tolerados respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
RR 3.3	Iniciar planes de respuesta a incidentes	1. Horas de capacitación y formación de responsables de la gestión y el riesgo de la empresa, en el logro de las mejores respuestas de cada incidente y el uso del CMS de la organización para ello respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		2. Horas de reuniones en charlas formales e informales y benchmarking para lograr las mejores respuestas a incidentes y correcta distribución del conocimiento a los interesados respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		3. Existencia de una base de conocimiento actualizada con categorías de hechos y respuestas.	Existe	No Existe

	Proceso	Indicador	Valoración Empresa informática	Valoración Inmobiliaria
RR 3.4	Comunicar las lecciones aprendidas de eventos de riesgo	1. Horas de capacitación y formación de responsables de TI y del riesgo de la empresa, en la identificación de las causas de problemas respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		2. Horas de capacitación en charlas, grupos de expertos y benchmarking sobre identificación de causas de problemas respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	0-5%
		3. Existencia de un CMS actualizado con datos históricos y recientes de acontecimientos adversos y pérdidas.	Existe	No Existe

5.3. Conclusión y Evaluación

Se puede observar como resultado de la experimentación que la empresa informática cuenta con un 56 % de los indicadores en el nivel 1, 43,2 % en el nivel 2 y 0,8 % en el nivel 3. Es por ello que se ubica en el nivel 1 del modelo de madurez. La empresa cuenta con aproximadamente la mitad de los procesos ponderados en niveles mayores al nivel inicial.

Discriminando el porcentaje de indicadores por nivel en cada dominio de gestión del riesgo, se observa la siguiente distribución:

Figura 17 Porcentaje de indicadores en cada dominio según su nivel en el modelo

Dominio de Gestión del Riesgo	Nivel del Modelo	Porcentaje de Indicadores en el Dominio
Proceso Gobierno del Riesgo (RG)	1	46,5
	2	53,5
Proceso Evaluación del Riesgo (RE)	1	47,6
	2	50
	3	2,4
Proceso Respuesta del Riesgo (RR)	1	45
	2	55

Los distintos dominios presentan una distribución similar dentro de los niveles del modelo. Particularmente en el dominio de Evaluación del Riesgo, existen indicadores en un nivel 3, con un grado de avance mayor respecto al resto.

En el caso de la empresa inmobiliaria, el 100% de sus indicadores corresponden al nivel 1 del modelo. La existencia de un evento pasado que genere la pérdida de información relevante para la empresa, puede ser un elemento motivador para el compromiso de los integrantes de la misma, en la búsqueda de la gestión del riesgo.

En la búsqueda de la mejora en la gestión del riesgo en base a la gestión del conocimiento en las empresas; se propone avanzar en el acceso al siguiente nivel del modelo, con una inversión mínima, que requerirá de un compromiso mayor de la dirección y de los RRHH en general, para el logro de estas mejoras [Anexo VI].

Teniendo en cuenta que se destacan los RRHH y compromiso de la dirección como los factores de éxito más relevantes para la implementación de una mejora en la gestión del riesgo basada en la gestión del conocimiento, indicados en el Anexo VI, basado en encuestas realizadas a PyMEs de Uruguay, se debería avanzar en la búsqueda de un mayor compromiso y creación de una cultura organizacional en gestión del riesgo y conocimiento.

A su vez, para el logro de este objetivo se pueden definir prácticas con un nivel de inversión asociado mínimo, requiriendo básicamente el compromiso de los RRHH en su realización, como ser reuniones y charlas informales y formales, para tratar los temas asociados a la identificación de riesgos y sus categorías, escalas y jerarquías, definición de umbrales y creación de un plan de comunicación de riesgos, así como definición de planes de capacitación en estos temas, con la participación activa de la dirección, logrando así una mejora del 41 % de los indicadores respecto al total de indicadores de nivel 1 en la empresa informática, mientras que sería de un 34 % para la inmobiliaria.

Por otra parte, en la empresa informática, dado que cuenta con bases de conocimiento y mapas ajustados a determinados temas en gestión del riesgo, se sugiere analizar, la inclusión de nuevos elementos en los mapas y bases de conocimiento que sustenten los ítems aún no definidos determinados como pendientes o con un grado de avance insuficiente para el nivel objetivo, como resultado de la encuesta realizada, con lo cual se logrará superar un 20 % de los indicadores respecto al total de indicadores de nivel 1.

Para lo que se sugiere hacer uso de técnicas de gestión del conocimiento como reuniones y charlas formales e informales, que faciliten la inclusión de los nuevos ítems a las bases y mapas de conocimiento existentes, logrando a su vez, un involucramiento mayor de los recursos humanos y promoviendo una cultura organizacional en gestión del conocimiento y el riesgo.

Para mejorar en los restantes indicadores, si bien pueden requerir una inversión mayor, pueden implementarse de tal forma que se minimice la inversión requerida, como es el caso de la capacitación, formación y charlas con expertos, donde se plantea realizarlo a grupos reducidos. De esta forma se reducen los costos en horas destinados a capacitación y formación por parte de expertos en cada tema, permitiendo luego que los recursos que fueron capacitados diseminen el conocimiento adquirido al resto de los recursos de la empresa, reduciendo la inversión asociada a este ítem.

Se debería definir la figura del CKO, para la cual se podría implementar la misma de forma que sea un rol asignado a un integrante de la empresa en forma no exclusiva y con una

capacitación inicial que no implique una inversión importante. A su vez, también se debería de implementar la utilización de sistemas expertos en la asignación de recursos que facilite la gestión.



Figura 18 Indicadores por categoría y nivel para la empresa informática

Para el caso de la empresa inmobiliaria, dado que el grupo de trabajo es reducido, podría no ser necesario contar con mecanismos de diseminación del conocimiento, capacitando y formando directamente a todo el personal. La empresa si bien esta en el nivel 1 al igual que la empresa informática, la misma cuenta con todos sus indicadores en el mismo nivel (nivel 1), debiendo realizar un esfuerzo mayor para alcanzar el siguiente nivel en el modelo.

Analizando la complejidad en la implementación de cada indicador, según la categorización de indicadores básicos o avanzados presentada anteriormente al definir los indicadores, podemos determinar el grado de esfuerzo requerido para el paso al siguiente nivel del modelo, basado en la complejidad del indicador y su grado de avance en la empresa (nivel alcanzado).

En el caso de la empresa inmobiliaria la totalidad de los indicadores se encuentran en el nivel 1. Por lo cual se tendría la siguiente gráfica:

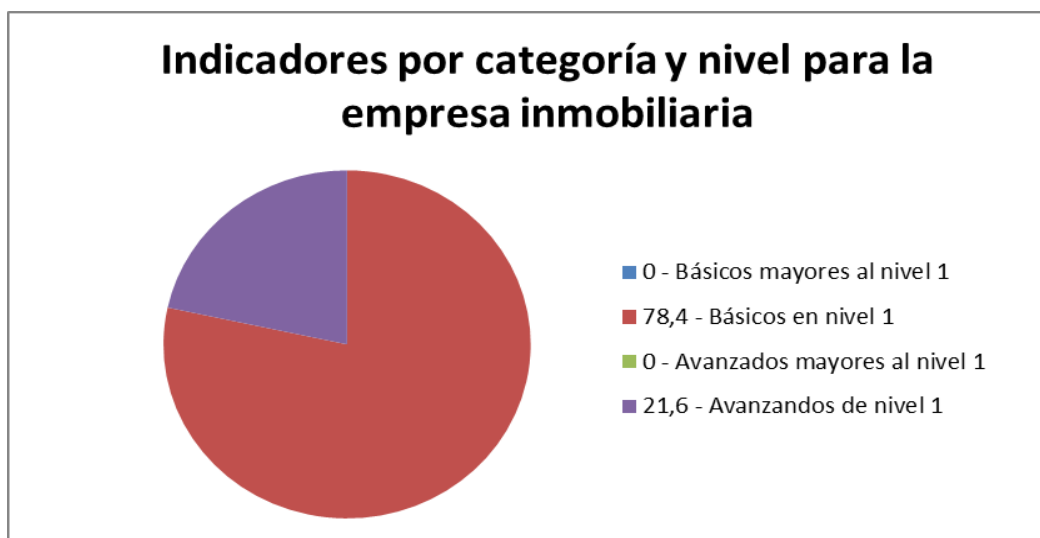


Figura 19 Indicadores por categoría y nivel para la empresa inmobiliaria

Podemos observar que las PyMEs presentan dificultades en la gestión del conocimiento para la gestión del riesgo (las empresas relevadas se ubican en el nivel 1 del modelo) y pueden

mejorar con una inversión baja o media, obteniendo una mejora sustantiva en su nivel dentro del modelo y por tanto en la gestión del riesgo en la organización [Anexo V].

En general, si agrupamos los indicadores en 5 categorías (Involucramiento de la dirección y recursos humanos de la empresa, Definición de mapas y bases de conocimiento, Capacitación, formación y charlas con expertos, Definición de un CKO y Aplicación de sistemas expertos) a las cuales se les puede asociar un nivel de inversión que definimos en los rangos Bajo, Medio y Alto, pudiendo existir categorías que en base a la forma y profundidad de su aplicación podrían pertenecer a más de un rango de costos, se implementa la siguiente Figura 18, donde se detallan las categorías y sus costos asociados, así como su impacto en el modelo (% máximo de mejora).

Se observa que las PyMEs pueden acceder al nivel siguiente del modelo (mejora en un 36%) por medio de procesos que implican un mayor involucramiento en la gestión del riesgo por parte de la dirección y el conjunto de los recursos humanos de la empresa, que implica una mejora en la gestión del riesgo (6.11), lo cual implica un costo mínimo, ya que requiere básicamente del compromiso y disposición en la mejora de la gestión del riesgo por parte de los recursos humanos.

Figura 20 Porcentaje de mejora en el modelo y costo asociado por categoría de los indicadores

Categoría	Costo	% de mejora
Involucramiento de la dirección y recursos humanos de la empresa	Bajo	36
Definición de mapas y bases de conocimiento	Medio	36
Capacitación, formación y charlas con expertos	Medio / Alto	26.4
Definición de un CKO	Medio / Alto	0.8
Aplicación de sistemas expertos	Medio / Alto	0.8

A su vez, la definición de mapas y bases de conocimiento, que requieren mayormente de un compromiso en su definición y dedicación en la elaboración y mantenimiento de los mismos, generaría una mejora sustantiva en el avance al siguiente nivel del modelo, mejorando hasta un 36% según los indicadores definidos, avanzando así en la identificación, incorporación, preservación y diseminación del conocimiento disponible en la organización (6.11).

Se puede concluir que la mejora en la gestión del riesgo basada en la gestión del conocimiento puede ser implementada en las empresas PyMEs con una inversión y grado de esfuerzo mínimos, obteniendo mejoras relevantes (mayores al 70 %), permitiendo así su avance a niveles superiores en el modelo, lo cual implicaría una mejora en la gestión del riesgo en la empresa [Anexo V].

6. Conclusiones y trabajo futuro

Según lo presentado en el [Anexo III] y por lo observado en la experimentación para las empresas encuestadas, 2 de 3 organizaciones de tipo PyMEs se ubican en un nivel bajo de madurez.

Es así que mediante la experimentación se aplicó el modelo de gestión del riesgo basado en gestión del conocimiento, llegando a definir un nivel para las empresas relevadas respecto a este modelo, permitiendo identificar las mejoras a realizar en cada caso, aplicando cambios que se pueden considerar de menor o mayor inversión, que facilitan y permiten minimizar los costos asociados a la mejora a realizar. Aplicando medidas prácticas de seguridad que no requieren mayor inversión más que informarse sobre algunos marcos de trabajo (libres y gratuitos en algunos casos como COBIT y VALIT), entre otras medidas de mejora sugeridas. De esta forma se logrará la aplicación de buenas prácticas en los primeros niveles logrando un cambio directo en lo que a gestión del riesgo refiere.

El marco diseñado y aplicado en la experimentación no contempla todos los ítems de los marcos y estándares utilizados como referencia para la creación del mismo. Esto es debido a que no todos los procesos aplican al contexto de empresas de tipo PyMEs dada su estructura y características, indicando la diferencia existente en la gestión del riesgo que se puede aplicar a empresas de este tipo respecto del resto.

Este marco y modelo fue diseñado siguiendo como base el planteo del trabajo presentado en (1), en el cual se toman los procesos de COBIT y VALIT como guía de la definición del marco. Dado que en dicho trabajo se realizan excepciones, no contemplando algunos de sus procesos, por no aplicar al contexto de las PyMEs para las cuales se define el mismo, dichas excepciones también aplican al presente marco.

Por tanto, los procesos del marco COBIT que no aplican en este trabajo son el monitoreo de tendencias y regulaciones futuras, que no se ajustan a estas empresas dada la estructura de TI de las mismas, así como recursos económicos y humanos requeridos para considerarlos. Otro proceso es el de contar con un consejo de arquitectura de TI, un comité estratégico y un comité directivo de TI, que implican costos excesivos que no se ajustan a la realidad de las PyMEs (Anexo III).

De igual forma los procesos de VALIT de establecer estructuras organizativas, evaluar casos de negocio de concepto de programa inicial, evaluar y asignar puntuaciones relativas al caso de negocio del programa, adquirir un claro entendimiento de los programas candidatos y desarrollar un caso de negocio detallado del programa, no aplican en este modelo ya que las PyMEs no cuentan con recursos económicos y humanos requeridos para su implementación o estructuras que permitan definirlos, por ser procesos muy amplios y detallistas, así como difícilmente tercerizables por el grado de conocimiento requerido sobre la organización a la cual aplican (Anexo III).

A su vez, de la experimentación realizada, se deduce que los pasos a seguir deben buscar el involucramiento de los recursos humanos así como el compromiso de la dirección, considerados factores de éxito de mayor impacto. Aplicando herramientas y técnicas que no fueran aprovechadas en la empresa, como ser grupos de expertos, círculos de calidad, lecciones aprendidas, así como clasificación y clustering, las cuales fueron detectadas como de menor nivel de adecuación en las encuestas realizadas a PyMEs de Uruguay, fortaleciendo las etapas de gestión del conocimiento de mayor dificultad en su implementación, como ser la retención, identificación y adquisición (Anexo V)

Aplicando estas técnicas en los distintos aspectos de la gestión del riesgo, principalmente en aquellas donde se presenta mayor dificultad, que según lo relevado serían la evaluación del riesgo y respuesta al riesgo (Anexo V).

Estos cambios sugeridos se ajustan a los resultados obtenidos en el estudio de campo realizado y desarrollado en el Anexo I, donde se propone incorporar buenas prácticas de inversión mínima y de inversión mediana que mejoran sustantivamente la gestión del gobierno de TI en el contexto de las pequeñas y medianas empresas, que en particular implica una mejora en la gestión del riesgo. En dicho trabajo se plantea una mejora en la gestión de riesgos que permitiría una mejora en la gobernanza de TI de un 70% de las organizaciones, también se plantea que una reducción en la falta de conocimiento en cuanto al uso de buenas prácticas de TI, mejoraría la gobernanza en un 90% de las organizaciones.

Por tanto, luego de la experimentación se plantea realizar la implementación de los cambios sugeridos, aplicados a las empresas evaluadas, realizando al término de un período de tiempo de 6 meses o un año, una nueva evaluación del estado de dichas empresas, en base al modelo, mediante un proceso de experimentación similar al realizado en la etapa inicial de evaluación, permitiendo así medir el grado de avance logrado con los cambios aplicados, determinando el impacto de los mismos.

En particular, la empresa informática encuestada, ha realizado cambios según lo sugerido, trabajando en la inclusión de ítems a las bases y mapas de conocimiento existentes, así como promoviendo el mayor involucramiento de los recursos humanos y dirección en la gestión del riesgo, observando un grado de compromiso creciente en su personal, que implica un factor a favor de la formación de una cultura organizacional en gestión del conocimiento y el riesgo en la empresa.

Se busca encontrar un mecanismo sistemático de evaluación, mejora y medición de avance respecto a la gestión del riesgo, según su gestión del conocimiento. Observamos en base a la información obtenida de la experimentación, que el marco y modelo permitirán encontrar un proceso sistemático, aplicable a empresas PyMEs en general, extendiendo o generalizando el procedimiento aplicado, que podrá ser implementado por algún producto de software que facilite el relevamiento, sugiera los cambios a realizar y su posterior medición de avance, al término de su aplicación. Este producto permitirá gestionar la información en tiempo real sobre las distintas características a medir, que permitirá monitorear el avance y cumplimiento de los pasos a seguir para avanzar en los niveles de madurez de la organización.

Este producto pasaría a formar parte de las herramientas de gestión de la empresa para la toma de decisiones, que permitiría visualizar el estado de cada área o sector pudiendo advertir sobre posibles amenazas o debilidades. A su vez, brindaría indicadores en tiempo real que se utilizarían dentro de los procesos de gestión la organización, integraos a éstos, lo que propicia un mayor involucramiento de los recursos humanos así como de la dirección, considerados factores de éxito según la experimentación realizada. Este involucramiento de los recursos humanos así como el uso de la herramienta, colaborará en la generación de una cultura de gestión del riesgo y conocimiento en la organización, facilitando la concreción de la mejora en la gestión del riesgo y conocimiento. Sugiriendo a cada área o sector, las herramientas y técnicas de gestión del conocimiento que mejor se ajusten para su aplicación, generando una mejora de costo mínimo, aplicado a los procesos de gestión del riesgo que requieran mayor control para minimizar los riesgos del área o sector en la empresa. Logrando de esta forma un producto que habilite la sistematización y gestión del conocimiento aplicado a la gestión del riesgo, que permita una mejora cuantificable y cualitativa en este aspecto.

El producto podrá ser evaluado en PyMEs de Uruguay y otros países, permitiendo verificar su aplicabilidad a realidades variadas, con culturas diversas, que permitirá determinar el grado de ajuste y generalidad del modelo y producto.

7. Referencias

- (1) Garbarino, H., “Marco de Gobernanza de TI para empresas PyMEs - SMEsITGF,” Tesis Doctoral, Facultad de Informática, Universidad Politécnica de Madrid, Madrid, España, 2014.
- (2) Ayala, S., “Características y estado de la Gestión del Conocimiento en las PyMEs del Uruguay”, Investigación para tesis de maestría, Universidad ORT, Montevideo, Uruguay, 2014
- (3) Basili , V; Schneider, K ; Von Hunnius, J. Experience in Implementing a Learning Software Organization. En IEEE Software [online] pp. 46-49, jun.2002. [citado 15 Noviembre 2012]. Disponible en Internet: <http://www.cs.umd.edu/~basili/publications/journals/J85.pdf>
- (4) ITGI, CobiT© 4.1, 2007, ISACA: USA.
- (5) ISACA, COBIT® 5 Tool Kit, 2012.
- (6) IT_Governance_Institute, Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, 2008, ISACA: USA.
- (7) Baig, K., ITIL Foundations Certification Course.
- (8) ISO/IEC, ISO/IEC 38500:2015. Corporate Governance for Information Technology., 2015, ISO.
- (9) Calder, A., The Calder-Moir IT Governance Framework. 2008.
- (10) MICROSOFT CORPORATION. 2008. MOF Version 4.0. [online] [3 de julio] Disponible en Internet : <[http:// www.microsoft.com/mof](http://www.microsoft.com/mof) >
- (11) ITGI, Marco de riesgos de TI. Risk IT, 2009, ISACA.
- (12) DINAPYME, Criterio de clasificación de Empresas en el Uruguay, in, 1995.
- (13) DINAPYME, Estructura de las Empresas PYMES en el Uruguay, in: MIEM (Ed.) Observatorio PYME Uruguay, 2005.
- (14) U. DINAPYME, Teresa Herrera & Asociados Consultoría, Encuesta Nacional de Pymes industriales y de servicios, (2008).
- (15) C. Scaronne, La informalidad en las MIPYMES de Uruguay. Análisis de los costos de la formalidad, Ministerio de Industria, Energía y Minería, Montevideo, Uruguay, 2007.
- (16) [on-line][9 Abril 2015] Disponible en Internet: <<http://www.sba.gov/>>

- (17) N. Malhotra, Investigación de mercado, Prentice-Hall, Georgia, 2004.
- (18) WEILL, Peter; ROSS, Jeanne. 2004. IT Governance. Boston: Harvard Business School Publishing
- (19) Cadbury, Report of the Committee on the Financial Aspects of Corporate Governance, 1992: London.
- (20) OCDE, Principios de Gobierno Corporativo de la OCDE, 2004, Organización para la cooperación y el desarrollo económicos: París.
- (21) CAF, Lineamientos para un Código Andino de Gobierno Corporativo. Eficiencia, equidad y transparencia en el manejo empresarial, 2006.
- (22) IFC, Gobierno corporativo. Demostrar la importancia de un mejor gobierno corporativo, 2008: Washington, USA.
- (23) ITGI, ed. IT Governance Global Status Report—2008. 2008, ISACA: United States of America.
- (24) Diamond, A. Gobierno Corporativo. in IX Congreso Latinoamericano de Auditoria Interna y Administración de Riesgos 2005. 2005. Panamá.
- (25) Wolfensohn, J.D., A Corporate Governance Approach Statement by Development Finance Institutions, 2007, The World Bank.
- (26) BCU, Estándares mínimos de gestión para instituciones de intermediación financiera, Superintendencia_de_Servicios_Financieros, Editor 2009: Montevideo, Uruguay.
- (27) Australian Corporate Governance. A review and Analysis and Key Issues: Pearson, Australia, 2013.
- (28) Weill, P. and J. Ross, IT Governance. How top performers manage IT decision rights for superior results, 2004, Harvard Business School Press: Boston, Massachusetts.
- (29) Toomey, M., Waltzing with the Elephant: A comprehensive guide to directing and controlling information technology., ed. Infonomics_Pty_Ltd.2009, Australia: Infonomics.
- (30) Weill, P. and J.W. Ross A Matrixed Approach to Designing IT Governance. 2005.
- (31) Walton, M., El método Deming en la práctica2004, Bogotá: Editorial Norma.
- (32) Deming, E.W., The New Economics. For Industry, Government, Education. 2nd. ed1994, Massachusetts: The MIT Press.
- (33) Deming, E.W., Calidad, Productividad y Competitividad. La salida de la crisis1989, Madrid: Editorial Díaz de los Santos.
- (34) ITGI Board Briefing on IT Governance. 2003.

- (35) Cuevas, G., J. Calvo-Manzano, and M. Muñoz, Process Similarity Study: Case Study on Project Planning Practices Based on CMMI-DEV v1.2.
- (36) OCDE, Principios de la OCDE para el gobierno de las sociedades 1999.
- (37) Calder, A., The IT Governance Toolkit-v05, 2008, IT Governance Publishing.
- (38) Guldentops, E., Governance of IT in Small and Medium Sized Enterprises, in Information Systems for Small and Medium-Sized Enterprises. State of Art of IS Research in SMEs, J. Devos, H. van Landeghem, and D. Deschoolmeester, Editors. 2014, Springer-Verlag: Berlin Heidelberg.
- (39) van Bon, J., M. Pieper, and A. van der Veen, Foundations of IT service management based on ITIL. 2nd ed. ITSM library, ed. J. van Bon, M. Pieper, and A. van der Veen 2005: Zeewolde: Van Haren,.
- (40) ITGI and OGC Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa. 2008
- (41) IT GOVERNANCE INSTITUTE. 2014. ISO/IEC 27000. Rolling Meadows: ISACA
- (42) Kaplan, R.S. and D.P. Norton, eds. The Balanced Scorecard. 1996, Harvard Business School Press: Barcelona.
- (43) Van-Grembergen, W., The Balanced Scorecard and IT Governance. Information Systems Control Journal ISACA, 2000. 2.
- (44) Van-Grembergen, W. and S. De-Haes, Enterprise Governance of Information Technology. Achieving Strategic Alignment and Value 2009, New York: Springer
- (45) Van-Grembergen, W. and De_Haes, Measuring and improving IT governance through the balanced scorecard. Information System Control Journal, 2005. 2: p. 35.
- (46) Samuwai, J., J. Heales, and A. Prasad, Towards an Effective IT Governance Structure for Organizations in Developing Economies, in 18th Americas Conference on Information Systems 2012: Seattle.
- (47) Stanford, C. Gartner Says Worldwide IT Spending to Grow 5.1 Percent in 2011. 2011; Available from: <http://www.gartner.com/it/page.jsp?id=1513614>.
- (48) Heeks, R., Information Systems and Developing Countries: Failure, Success, and Local Improvisations. The Information Society, 2002. 18(2): p. 101-112.
- (49) Raymond, L., Organizational Characteristics and MIS Success in the Context of Small Business. MIS Quarterly, 1985. 9(1): p. 37-52.
- (50) Ayala, S, Rebuffel, A. (2010): Alineamiento Estratégico de TI en Pymes del Uruguay, Proyecto de Grado, Universidad ORT Uruguay
- (51) SEI. 1993. CMM. V1.1. USA: Universidad Carnegie-Mellon.

- (52) T.Davenport, L. Prusak,L, Working knowledge: how organizations manage what they know (Bookstyle). Boston, MA: Harvard Business School Press, 1998, pp. 1-25
- (53) G.Probst, S.Raub, K.Romhardt, Administre el conocimiento (Bookstyle), México D.F, México: Pearson, 2001, pp. 1-20.
- (54) K.Wiig, Knowledge management foundations (Bookstyle), Arlington, USA, Schema Press, 1993, pp. 1-30.
- (55) A.Gomez, N.Juristo, C.Montes, J.Pazos, Ingenieria del conocimineto (Bookstyle), Madrid, España: Centro de Estudios Ramón Areces, S.A, 1997, pp. 43-87.
- (56) M. Alavi, Managing organizational knowledge (Bookstyle), Cincinnati, USA: Pinnaflex Educational Resources, 2000, pp. 15-28.
- (57) A. DelMoral, J. Pazos, E. Rodriguez, A, Rodriguez-Paton, S. Suarez, Gestion del conocimiento (Bookstyle). Madrid, España: Paraninfo, 2007.
- (58) L.Paradela, “Una metodología para la gestión del conocimiento,” Tesis Doctoral, Facultad de Informática, Universidad Politécnica de Madrid, Madrid, España, 2001.
- (59) Morten T. Hansen, Nitin Nohria, Thomas Tierney, What’s Your Strategy for Managing Knowledge? Harvard Business Review, March-April, 1999.
- (60) Koskinen, K. Tacit Knowledge as a Promoter of Success in Small Technology Firms, St. Jerome Publishing, Manchester, 2001.
- (61) Gupta, J; Sharma, S. Creating Knowledge Based Organizations, Hershey, Idea Group, 2004
- (62) Alavi, M; Leider, D. Knowledge Management and knowledge Management Systems: Conceptual Foundations and Research Issues, Working papers: Battelle Press, Columbus Ohio, 1999.
- (63) Quintas, P., Lefrere, P. y Jones, G. (1997): “Knowledge management: a strategic agenda”. Long Range Planning, Vol. 30, nº 3, pp. 385-391.
- (64) tom davenport [on-line] [12 Diciembre 2014] Disponible en Internet: <<http://www.tomdavenport.com/>>
- (65) Prof. Gilbert Probst Organisation & Management [on-line] [12 Diciembre 2014] Disponible en Internet: <<http://probst.unige.ch/>>
- (66) LaurencePrusak.com [on-line][12 Diciembre 2014] Disponible en Internet: <<https://www.laurenceprusak.com/>>.
- (67) Davenport, T; Prusak,L. Working knowledge: how organizations manage what they know. Boston, MA: Harvard Business School Press, 1998
- (68) Nel M. Mostert, Hilbert J. Bruins Slot, Creativity, the knowledge Connector, Boston: Elsevier Butterworth-Heinemann, 2005.
- (69) Unilever Annual Report: Unilever, 2002.

- (70) Martin, J. Eppler, Making Knowledge Visible through Knowledge Maps: Concepts, Elements, Cases. International Handbook on Information Systems, 2004.
- (71) Nataya Noy, Deborah Mc Guinness. "Ontology Development 101: A Guide to Creating Your First Ontology", Stanford University, Stanford, CA.
- (72) Minsky, M. "A Framework for Representing Knowledge" Editorial P. Winston. McGraw-Hill. New York, EE.UU. 1975.
- (73) Asunción Gómez, Natalia Juristo, César Montes, Juan Pazos. "Ingeniería del Conocimiento". Editorial Centro de Estudios Ramón Areces, S.A. 1997.
- (74) A.J. Arroyo, J.D. Carrillo, The status of IT Governance in Spanish organizations. Analysis and conclusions for identifying best practices, in, 2009.
- (75) BCU, Instituciones de intermediación financiera - Normativa sobre gobierno corporativo y sistema de gestión integral de riesgos., in, 2008.
- (76) M. Bunge, La Ciencia Su Método Y Su Filosofía, Eudeba, Buenos Aires, 1960.
- (77) ESADE, Corporate Governance, el buen gobierno de la empresa, in: EGuíame!, la Caixa, 2004.
- (78) Fundatec, Análisis sectorial de implantación de las TIC en la pyme española, in: I.P. 2008 (Ed.), 2008.
- (79) ISO, ISO/IEC 38500:2008. Corporate Governance for Information Technology., in, ISO, 2008.
- (80) ITGI, Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, in, ISACA, USA, 2008.
- (81) ITGI, COBIT® 5 Design Paper Exposure Draft, in, ISACA, 2010.
- (82) E.B. Sánchez, La investigación científica: Teoría y metodología, in, Zacatecas, 2003.
- (83) C. Symons, IT Governance Framework. Structures, Processes, And Communication, in: C.S.-. Forrester (Ed.), 2005.
- (84) I. Terán, Inversión en TI: Un partner cada vez más importante para la PYME Latinoamericana, in: InfoWeek, 2009.
- (85) W. Van_Grembergen, S. De_Haes, An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment, Information Systems Management, 26 (2007) 123-137.
- (86) P. Weill, J. Ross, Four Questions Every CEO Should Ask About IT, in: The Wall Street Journal, 2011.
- (87) U. DINAPYME, Equipos Mori, Consultores Asociados, "Encuesta Nacional de mPyMEs industriales y de servicios," 2013.
- (88) H. Mintzberg, Diseño de organizaciones eficientes. Buenos Aires: El Ateneo, 1989.

- (89) Petticrew, M. and H. Roberts, *Systematic reviews in the social sciences. A practical guide*, 2006, Malden, MA: Blackwell.
- (90) Kitchenham, B.A., D. Budgen, and O.P. Brereton, Using mapping studies as the basis for further research. A participant- observer case study. *Information and Software Technology*, 2011. 53: p. 638–651.
- (91) Petersen, K., et al., *Systematic Mapping Studies in Software Engineering*, in 12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 2008: Bari, Italy.
- (92) Arksey, H. and L. O'Malley, Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology*, 2005. 8(1): p. 19-32.
- (93) Auster, E., K. Wylie, and M. Valente, *Strategic Organizational Change. Building Change Capabilities in your Organization*, 2005, Hampshire: Palgrave Macmillan.
- (94) Gerhardt, M., D. Frey, and P. Fischer, The human factor in change processes: Success factors from a socio-psychological point of view, in *Change 2.0. Beyond Organisational Transformation*, J. Klewes and R. Langen, Editors. 2008, Springer: Berlin.
- (95) I. Nonaka and H. Takeuchi, *Modelo SECI*. Nueva York: USA: Oxford University Press, 1995.
- (96) T. Davenport, D. DeLong, and M. Beers, *Successful Knowledge management projects*. Boston, MA: Harvard Business School Press, 1998.
- (97) Chen Hongmei, Miao Yujun, *Knowledge Management for SMEs Based on the Balanced Scorecard*, Sch. Of Econ. & Manage., Qiqihar Univ., Qiqihar, China, 2010.
- (98) Qi Guiqing, Yang Xihuai, Xiao Zhuo, *Building the Competitive Advantage of SMEs in High-tech Industry on Knowledge Management View*, Sch. of Bus. Adm., Northeastern Univ., 2006.
- (99) R. Cross and L. Baird, "Technology is not enough: Improving performance by building organizational memory.", 2000.
- (100) Norkjaer, M.A., Scheel, H. ; Sorensen, M.A.S., *Why early implementation of a Knowledge Management System can support the growth of R&D-driven SMEs*, Inst. of Bus. & Technol., Univ. of Aarhus, Herning, Denmark, 2010.
- (101) Fang Luo, *Determinants of knowledge search strategy of Chinese SMEs*, Sch. of Manage., Zhejiang Univ., Hangzhou, China, *Industrial Engineering and Engineering Management (IEEM)*, 2010 IEEE International Conference on, 2010.
- (102) Nagi, K., *Use of moodle reports for knowledge management, planning and eTraining in SMEs*, Coll. of Internet Distance Educ., Assumption Univ., Bangkok, 2008.
- (103) M. Jennex, Olfman, L. , "Organizational memory/knowledge effects on productivity, alongitudinal study.", 2002.
- (104) E. Wenger, McDermott, R., Snyder, W. , "Cultivating communities of practice.", 2002.

- (105) Bandini, S., Manzoni, S. ; Sartori, F., Case-Based Reasoning to Support Work and Learning in Small and Medium Enterprises, DISCo Dept. of Comput. Sci., Syst. & Commun., Univ. of Milano-Bicocca, Milan, Italy, 2009.
- (106) Yuanhong Liao, Lili Qi, Knowledge Management System in Project-Based Organizations, Coll. Of Econ.&Manage., China Agric. Univ.(CAU), Beijing, China, 2009.
- (107) Portera-Zanotti, N. ; Rinsche, T., Innovative knowledge management practices for SMEs, Information Society (i-Society), 2010 International Conferenceon, 2010.
- (108) Noudoostbeni, A., Yasin, N.M. ; Jenatabadi, H.S., A Mixed Method for Training ERP Systems Based on Knowledge Sharing in Malaysian Small and Medium Enterprise (SMEs), Dep. Inf. Sci., Univ. Malaya, Kuala Lumpur, 2009.
- (109) Murni, H.F. , Siregar, L. ; Budiarto, R., Evaluating the Best of Knowledge Management Technology for Small Medium Enterprise Based on Fuzzy Analytic Hierarchy Process, Sch. of Comput. Sci., Univ. Sains Malaysia, Minden, 2009.
- (110) Abbaszadeh, M.A., Ebrahimi, M. ; Fotouhi, H., Developing a causal model of critical success factors for knowledge management implementation, Dept. of Ind., Persian Gulf Univ., Bushehr, Iran, 2010.
- (111) Mahmud, R., Rosnan, H. ; Hazman-Fitri, M.H., Knowledge management and innovation readiness among SMEs in Malaysia, Fac. of Bus. Manage., Univ. Teknol. MARA, Puncak Alam, Malaysia, 2013.
- (112) Trivedi, P., Dubey, A. Implementation of KM in Indian SMEs: modeling the variables, Amity Sch. of Eng. &Technol., Amity Univ., Lucknow, India, 2012.
- (113) MoonKoo Kim, JongHyun Park ; JongHyun Paik, An empirical analysis to strengthen the knowledge management capability in Korea SMEs, Future Strategy Res. Team, ETRI, Daejeon, South Korea, 2011.
- (114) Wei Long, Olufemi, E.A., Knowledge Management and Innovation for Firms Competitiveness: A Strategic Approach for African SMEs, Sch. of Econ., Wuhan Univ. of Technol., Wuhan, China, 2011.
- (115) Mesaric, J., Knowledge management - necessity and challenge in small and medium enterprises, Fac. of Econ., Univ. JJ. Strossmeyer, Osijek, 2004.
- (116) JingTian, Nakamori, Yoshiteru, Consideration on a service system for knowledge management in scientific laboratories, Sch. of Knowledge Sci., Japan Adv. Inst. of Sci. &Technol., Japan "2005.
- (117) Hamburg, I., eLearning 2.0 and Social, Practice-Oriented Communities to Improve Knowledge in Companies, Inst. for Work & Technol., FH Gelsenkirchen, Gelsenkirchen, Germany, 2010.
- (118) Beierle, Cristoph, Meghini, Carlo, Foundations of Information and Knowledge Systems, 8th International Symposium, Folks 2014, Proceedings Series of lecture notes in Computer Science., Bordeaux, France, 2014.

(119) P. Weill, J. Ross, Four Questions Every CEO Should Ask About IT, in: The Wall Street Journal, 2011.

ANEXOS

ANEXO I - Estudio empírico sobre los problemas de gobernabilidad de TI en empresas de tipo PyMEs y recomendaciones para mitigarlos

Caso de estudio: Uruguay

Helena Garbarino
Facultad de Ingeniería
Universidad ORT
Uruguay
Montevideo, Uruguay

Sebastián Ayala
Facultad de Ingeniería
Universidad ORT
Uruguay
Montevideo, Uruguay

José Carrillo
Facultad de Informática
Universidad Politécnica
de Madrid
Madrid, España

Resumen

El artículo tiene como objetivo presentar los resultados obtenidos en un estudio empírico acerca de la gobernanza corporativa de las tecnologías de la información realizado en la República Oriental del Uruguay a pequeñas y medianas empresas. Se presentan las principales debilidades encontradas y se establecen recomendaciones para mitigarlas. Se clasifican las recomendaciones según el grado de inversión que sea necesario realizar para implementarlas y se ponderan de acuerdo al grado de incidencia encontrado en el estudio.

Keywords: Gobierno Corporativo de TI, PyMEs, Alineamiento estratégico

Abstract

This article aims to present the results of an empirical study on Corporate Governance of Information Technology made in Uruguayan small and medium enterprises. It presents the main weaknesses identified and recommendations to mitigate them. These recommendations are classified after the level of investment needed to implement them and are weighted according to the degree of incidence found in the study.

Palabras claves

IT Corporate Governance, SMEs, Strategic alignment.

1. Introducción

El artículo tiene como objetivo presentar los resultados obtenidos en un estudio empírico acerca de la gobernanza corporativa de las tecnologías de la información (de aquí en más GCTI) realizado en la ROU a pequeñas y medianas empresas. Se mencionan y analizan las principales debilidades encontradas y se establecen recomendaciones para mitigarlas.

El artículo está organizado en nueve secciones, donde la primera es la introducción, en la segunda se define el contexto del gobierno corporativo y su historia, en la tercera sección se da contexto a las tecnologías de información, en la sección cuarta se define el contexto de las empresas PyMEs en la República Oriental del Uruguay, el contexto del Gobierno de TI y sus marcos así como las características e importancia de las pequeñas y medianas empresas en la economía uruguaya. En la sección quinta se presentan los objetivos del trabajo de campo presentando su metodología en la sección seis. Las secciones siete, ocho y nueve presentan los resultados obtenidos, los problemas más comunes y las conclusiones en donde se realizan una serie de recomendaciones para mitigar los problemas encontrados y una ponderación de los mismos según el grado de incidencia encontrado en el estudio.

2. Contexto del Gobierno corporativo

En los últimos años, escándalos y fraudes tales como los de Enron, Worldcom y Tyco (2002) entre otros han impulsado el desarrollo de códigos de buen gobierno corporativo que garanticen una gestión transparente, la estabilidad de los mercados financieros, la inversión y el crecimiento económico [16]. Estos códigos, leyes y modelos han evolucionado a lo largo del tiempo, distinguiéndose entre otros en Europa: el Informe Cadbury (Reino Unido, 1992); el Código Olivencia de Buen Gobierno (España, 1998); el Informe Winter: Report of the High Level Group of Company Experts on a Modern Regulatory Framework for Company Law in Europe (2002); el Informe Aldama (España, 2003); el Company Law and Corporate Governance y la Comisión Europa: Mercado Interior. A nivel internacional se destacan: el Principles of Corporate Governance: analysis and Recommendations (1992); los Principios de la OCDEb para el Gobierno de las sociedades (1999); el European Corporate Governance Institute; la Comisión Nacional del Mercado de Valores (España) y el código Sarbanes-Oxley (EEUU, 2002) (datos obtenidos del “Corporate Governance, Dossier de Recusos” [8]). En el Uruguay la entidad reguladora de dichos principios es el Banco Central del Uruguay a través del documento: “Instituciones de intermediación financiera - Normativa sobre gobierno corporativo y sistema de gestión integral de riesgos” cuya última versión es del año 2008 [2].

3. Contexto de las tecnologías de la información

La información y las tecnologías de la información (de aquí en adelante TI) forman parte del conjunto de activos clave en las organizaciones ya que habilitan la consecución de valor incidiendo tanto en aspectos internos como externos, en sus procesos, productos y comunicaciones, añadiendo valor a sus actividades y habilitando su eficacia y su eficiencia [11]. Esto se ve apoyado en los resultados empíricos obtenidos por los autores Weill y Ross los que han dado lugar al modelo propuesto por dichos autores y publicado en el libro “IT Governance. How top performers manage IT decision rights for superior results” [22].

Las organizaciones deben tomar cinco tipos de decisiones en lo que respecta a Tecnologías de la Información [22]:

1. Decisiones de principios de TI: son aquellas que establecen el rol de las TI en la compañía.
2. Decisiones de arquitectura de las TI: son aquellas que determinan las elecciones técnicas en TI.
3. Decisiones de infraestructura de TI: son aquellas que determinan la organización física de las piezas de hardware de la organización.
4. Decisiones de aplicaciones de negocio: son aquellas que determinan las especificaciones y requerimientos para las aplicaciones de negocio a desarrollar en la organización, que darán soporte a los procesos de negocio.
5. Decisiones de priorización y de inversiones en TI: son aquellas que determinan en que proyectos o recursos de TI invertir y que infraestructura adquirir.

Es muy importante que los directores de la empresa reconozcan la responsabilidad que tienen en la toma de decisiones y el uso y manejo efectivo de TI y no asuman que la responsabilidad es del departamento de TI, de aquí que, el ITGI, define al gobierno de TI como: “El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que TI en la empresa sostiene y extiende las estrategias y objetivos organizacionales”[11].

Las actividades de Gobierno de TI pueden ser agrupadas en las siguientes cinco áreas de enfoque, las cuales se detallan a continuación [11]:

- (1) **Alineamiento Estratégico.** Se enfoca en asegurar el enlace de los planes del negocio y de TI; en definir, mantener y validar la proposición de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa. Asegura que la inversión en TI de una empresa está acorde con los objetivos estratégicos de la misma.
- (2) **Entrega de Valor.** Se refiere a ejecutar la proporción de valor a través de todo el ciclo de entrega, asegurando que TI entrega los beneficios acordados alineados con la estrategia, concentrándose en la optimización de costos, y demostrando el valor específico de TI.
- (3) **Administración de Riesgos.** Se realiza a través de mitigar, transferir, aceptar y evitar. Para ello se requiere conciencia de riesgo por parte de los directores superiores de la empresa, entendimiento del apetito del riesgo de la empresa, transparencia sobre los riesgos significativos de la empresa e implementar las responsabilidades de la administración de riesgos dentro de la organización.
- (4) **Administración de Recursos.** Se refiere a la inversión óptima y la adecuada administración de los recursos críticos de TI (aplicaciones, información, infraestructura, personas).

(5) **Medición del Desempeño.** Da seguimiento y supervisa la estrategia de implementación, la finalización de proyectos, el desempeño de procesos y la entrega de servicio, ya que lo que no se puede medir, no se puede administrar.

De acuerdo con Peter Weill y Jeanne Ross [23] en una economía digital, las TI son la base de los negocios, por lo que, los CEOs o en el contexto de una empresa mediana, aquel que toma las decisiones debería preguntarse:

- ¿Estamos utilizando la tecnología para transformar nuestro negocio, o solo estamos agregando campanas y silbatos a los procesos existentes?
- ¿Estamos ignorando las diferencias importantes del negocio como estandarizar procesos en toda la empresa?
- ¿Quién se asegura que la estrategia digital de la compañía se está aplicando?
- ¿La información electrónica está capacitando a su personal o solo controlándolo?

Todos estos elementos hacen al contexto de las TI, su gobernanza y la obtención de valor a través de la misma.

4. Contexto de empresas PyMEs en la República Oriental del Uruguay

La realidad del mercado industrial en el Uruguay hace que las empresas categorizadas como PyMEs [5] tengan una incidencia fundamental; según la DINAPYME [6] el 99% de las unidades económicas productivas del sector privado del Uruguay son PyMEs y el 70% de las personas trabaja en empresas tipificadas como tales [7]. Esta particularidad hace que sea altamente relevante analizar elementos de gobierno de TI aplicados a este tipo de empresas. Éste tipo de empresa aporta el 33% de PBI y el 25% de la inversión [18].

También las PyMEs son muy importantes en las distintas economías del mundo. Estadísticas de la SBA de Estados Unidos muestran que en el 2007 las pequeñas empresas generaron alrededor del 50% de todas las ventas estadounidenses, y también contribuyeron al 50 % del PBI privado. Además, emplearon a más del 50% de la fuerza laboral de ese país [15].

4.1. Estado del arte del Gobierno Corporativo de TI

En conjunción con lo anterior, se han creado marcos de Gobierno Corporativo de las Tecnologías de la Información (de aquí en más GCTI) que garanticen el control de la información, la obtención de valor como consecuencia de la alineación estratégica entre los objetivos del negocio y los de TI, la gestión de los recursos y de los riesgos asociados a TI, así como la calidad de los servicios entregados.

Es en este sentido que surgen los siguientes marcos: los propuestos por el ITGI: el marco COBIT 4.1h [11], el marco Val IT [12] y el Risk IT [13-14], el marco propuesto por el CISR [22], el propuesto por Van Grenbergen [21], el ISO 38.500 [10], el marco Calder-Moire [4] y el marco Forrester [19].

Ejemplos comerciales como el publicado por InfoWeek [20], hace referencia directa a la importancia de las PyMEs en América Central y del Sur y de las inversiones en TI que las mismas realizan; en el ámbito europeo, el estudio realizado por el Aula TIC-PyMEs de la Universidad de Santiago de Compostela [9] donde se categoriza la importancia del uso de las tecnologías por tamaño/sector; otros estudios, como el realizado por Arroyo y Carrillo [1] respecto del uso de TICs y de la existencia/madurez de gobierno de TI en PyMEs españolas enfatizan la importancia de las TI y las debilidades existentes en la gestión de las mismas. Las características de las PyMEs les permiten mayor flexibilidad y mayor velocidad de respuesta frente a cambios en el sector donde se desarrollan, y es en éste sentido que la adopción de nuevas tecnologías puede contribuir a la obtención de mayores beneficios optimizando los procesos a lo largo de toda la cadena.

5. Objetivos del estudio de campo

El presente estudio no está enmarcado en ningún proyecto de carácter general ni gubernamental por lo que los objetivos del mismo son específicos al área y a la propia investigación. Los objetivos son: realizar un diagnóstico de la situación de la GCTI y a partir del mismo identificar los principales problemas y acciones para mitigarlos, dentro del contexto de pequeñas y medianas empresas en el Uruguay.

6. Metodología

Se analizaron 30 organizaciones entrevistando a Directores Generales, Directores Financieros, Directores de Departamento y Directores de TI de pequeñas y medianas empresas (hasta 100 trabajadores). La técnica utilizada fue la entrevista cara a cara, con una duración aproximada de 45 minutos.

Se definió una muestra no probabilística de criterio intencional [3], en la que el tipo de selección que primó es el criterio personal del investigador acerca de la representatividad y heterogeneidad de la población que se está estudiando. Por ello la selección incluyó una distribución heterogénea de rubros, tipos de empresas (industriales y de servicios), y zonas del país (departamentos de Montevideo, Maldonado, San José y Colonia) [17].

Margen de Error: No se puede calcular el error de la muestra por tratarse de una muestra no probabilística.

Sujeto Encuestado: Fueron encuestados Directores Generales, Directores Financieros, Directores de Departamento y Directores de TI de las empresas.

Unidad de Análisis: El análisis se centra en las PyMEs (pequeñas y medianas empresas).

Universo: El universo de análisis son las PyMEs (pequeñas y medianas empresas).

Procesamiento de la información Las encuestas fueron codificadas e ingresadas a una base de datos que se depura controlando inconsistencias. La información se procesó mediante un programa informático estadístico SPSS.

Alcance del Estudio El informe presentado corresponde a los resultados de la aplicación de la encuesta realizada durante los meses de julio – agosto de 2010.

Resultados de Campo: Del total de contactos efectuados, 100% constituyeron entrevistas efectivas, no existiendo ningún rechazo.

7. Resultados

A continuación se presentan los resultados obtenidos relativos a cada una de las áreas del gobierno de TI:

7.1. Gobierno de TI

En nueve de cada diez organizaciones no hay ningún conocimiento de Gobernanza de TI. Según estudio de madurez del alineamiento estratégico de TI en PyMEs de Uruguay que surge del presente estudio, el nivel de madurez de las PyMEs y el alineamiento estratégico de TI con los objetivos del negocio es el siguiente: 2 de cada 3 empresas (65%) está en los niveles 1 y 2 de madurez (la escala de niveles es de 1 a 5).

7.2. Toma de decisiones

En 1 de cada 2 organizaciones (50%) las decisiones de TI son tomadas únicamente por el gerente o director general y solo en un 2 % por el conjunto de directores de la empresa tal como podemos observar en la figura 1.

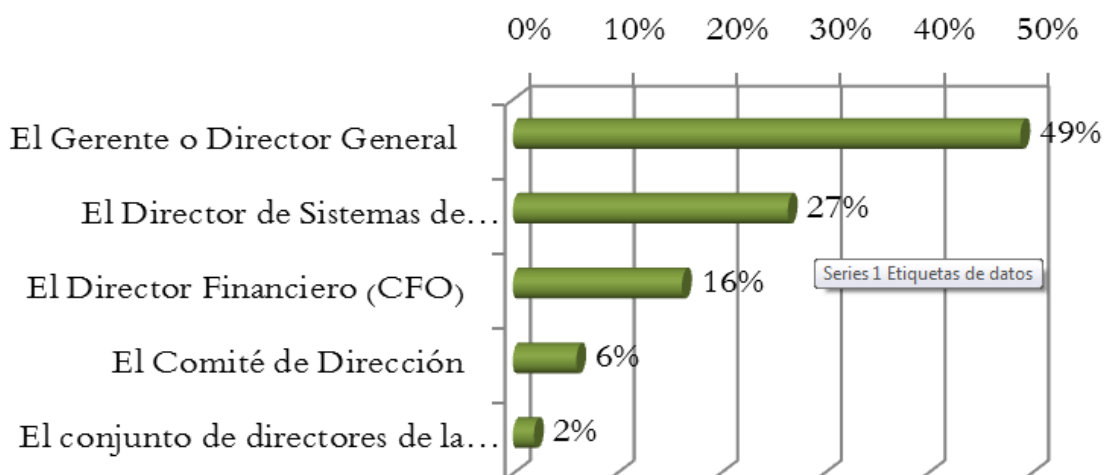


Figura 1. Toma de decisiones sobre TI

Sólo en 1 de cada 3 (33%) la planificación de la estrategia de TI es determinada con participación del director de sistemas y del director financiero además del director general como se muestra en la figura 2.

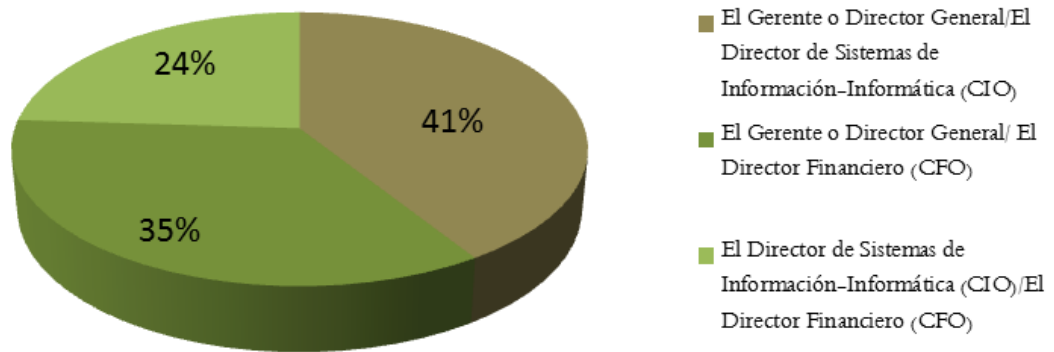


Figura 2. Responsable de la planificación de la estrategia de TI

7.3. Estructura de TI

En más de la mitad (54%) de las organizaciones no existe una estructura de TI definida que de soporte a los objetivos estratégicos de la organización y no existe alineamiento de TI con los objetivos del negocio de la organización.

7.4. Valor de TI

En la mayoría de las organizaciones (64%) se percibe a TI solo como un soporte operativo al negocio, no existiendo responsabilidades definidas en TI y no valorizando la importancia que tiene TI para apoyar y lograr el cumplimiento de los objetivos del negocio así como la mejora continua del mismo tal como se muestra en la figura 3.

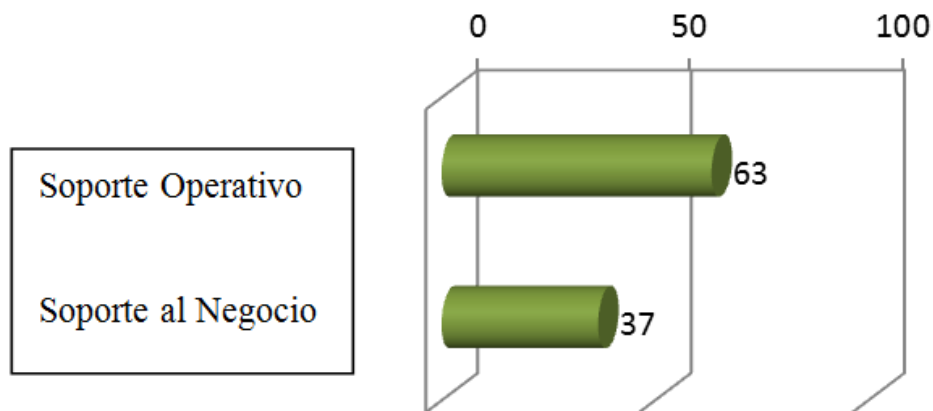


Figura 3. Soporte al negocio

En general no se corresponde la importancia que los empresarios dicen asignarle a TI como elemento que permite la consecución de una estrategia (65% la considera imprescindible) en relación a los gastos del presupuesto asignados a TI (47% le asigna entre un 5 y un 10%) tal como podemos apreciar en la tabla 1 y en la figura 4

Tabla 1. Presupuesto asignado a TI

% de presupuesto	% de casos
5	23,1
10	23,1
3	7,7
8	7,7
15	7,7
25	7,7
30	7,7
40	7,7
50	7,7

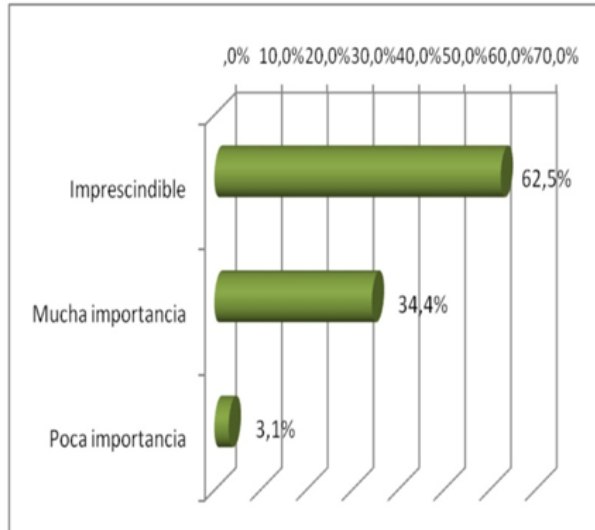


Figura 4 Importancia de TI en la organización

El 40% de las organizaciones no mide el valor que le aporta TI al negocio.

7.5. Riesgos y seguridad de TI

Solamente 1 de cada 3 organizaciones (30%) realizan una gestión de riesgos en el área de seguridad de la información.

El 70% de las empresas no cuenta con un plan de recuperación de desastres. El restante 30% se caracteriza por si poseer un plan de contingencia tal como podemos apreciar en la figura 5.

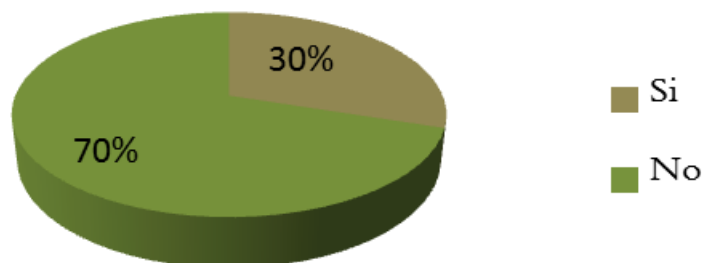


Figura 5. Existencia de un plan de recuperación de desastres

7.6. Servicios de TI

- La mayoría de las organizaciones (83%) no ha definido los servicios que TI debe brindar a la organización.
- La mayoría de las organizaciones (86%) no monitorea la calidad ni el cumplimiento de los servicios de TI.
- La mayoría de las organizaciones (93%) no han implementado acuerdos de tipo SLA para los servicios de TI.
- Ninguna de las empresas ha implementado acuerdos de tipo SLA para los servicios contratados a terceros.

8. Problemas más comunes

Falta de Conocimiento. El problema más relevante y común en todos los niveles es la falta de conocimiento de gobernanza de TI como podemos observar en la figura 7 y la no aplicación de buenas prácticas de gobernanza de TI como se representa en la figura 6; un 42% de las organizaciones expresa que no realiza prácticas de gobernanza y solo el 14% expresa que las realiza parcialmente.

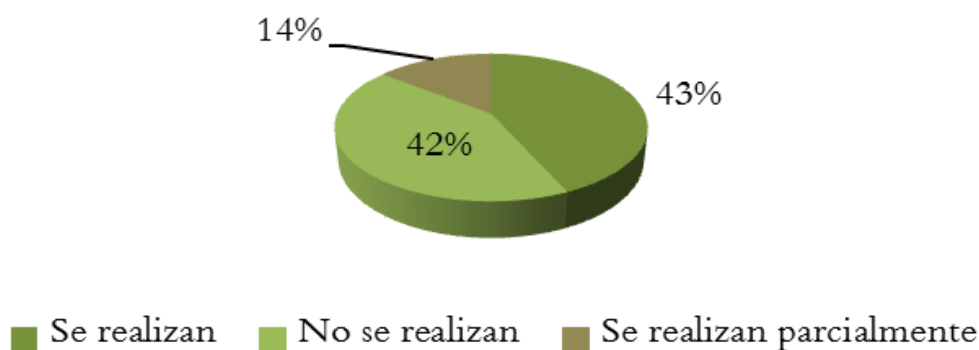


Figura 6. Realización de buenas prácticas de gobernanza de TI

Falta de Cultura organizacional. Es uno de los problemas más importantes que impiden que las organizaciones puedan avanzar en su madurez a través del conocimiento de TI y de las posibilidades que permite una buena gobernanza de TI (figura 7).

En general cuando las organizaciones aplican procesos y prácticas de gobernanza de TI o aplican un marco propio lo hacen por imposición de las marcas a las que representan para certificarse en alguna norma de calidad que les exigen las marcas para las cuales trabajan y no lo realizan con el objetivo de mejorar el alineamiento estratégico de TI con los objetivos del negocio.

Toma de decisiones no compartida. La participación conjunta del director general de la organización, el director de TI y los directores de los departamentos en la infraestructura, la toma de decisiones e inversiones de TI permite resolver los problemas de TI más frecuentes en las organizaciones. Esta participación conjunta no existe o es muy baja. En un 65% de las organizaciones no existe una participación conjunta en la definición de procesos, estructuras, y la planificación de los objetivos de TI (Figura 2) y en un 50% de las organizaciones quien toma las decisiones de TI es el director general. (Figura 1).

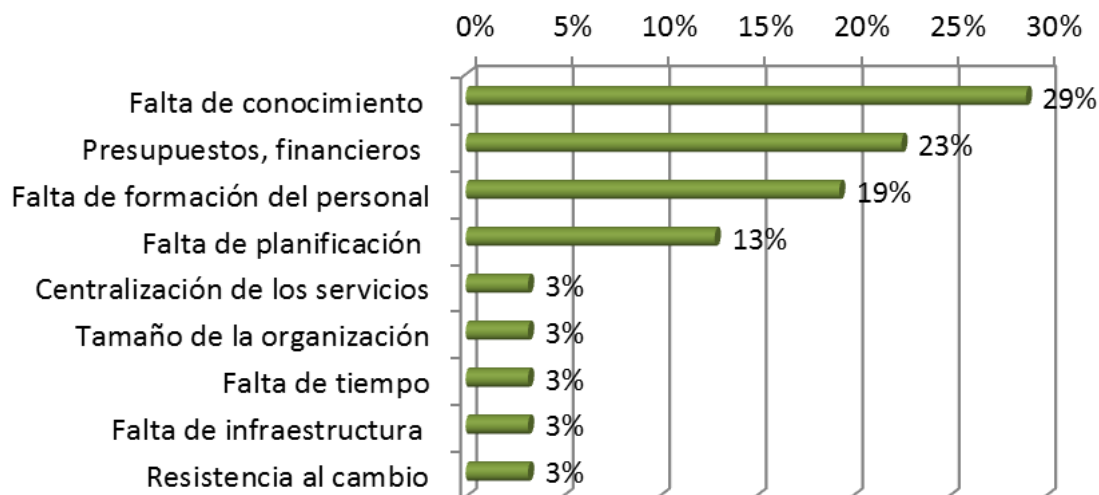


Figura 7. Obstáculos para que la organización no adopte buenas prácticas de gobernanza de TI

Problemas de gestión de riesgos y seguridad. Existe un gran problema en cuanto a la seguridad de la información y la gestión de riesgos en la mayoría de las organizaciones ya que estas no cuentan con sistemas de respaldos ni políticas de seguridad adecuadas, ni con un plan de contingencia y recuperación de desastres (70% de las organizaciones no cuenta con un plan de contingencia y recuperación de desastres (Figura 5)). No se dimensiona el problema que puede ocasionar la no disponibilidad o pérdida de la información. Solo un 30% de las empresas consultadas realiza una gestión de riesgo en el área de seguridad de la información como se muestra en la figura 8.

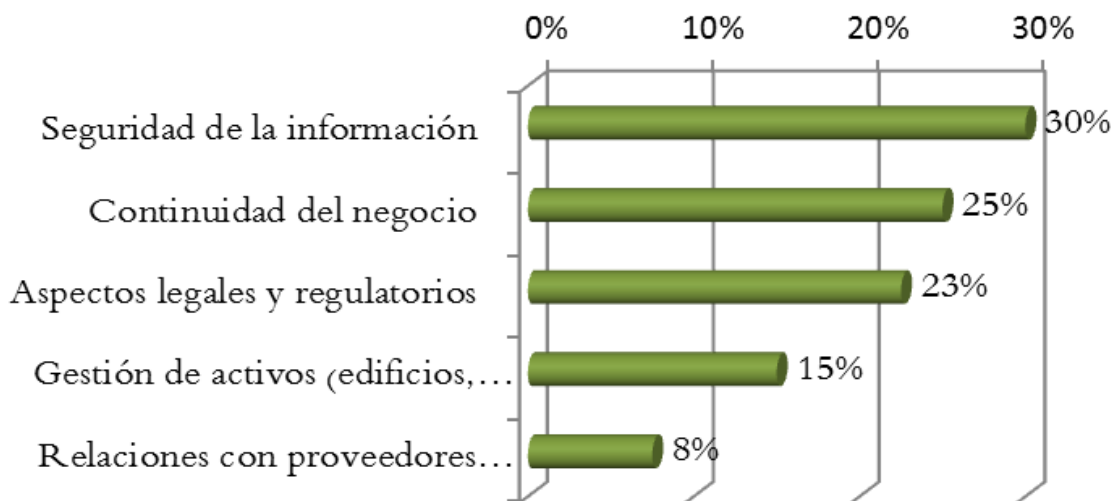


Figura 8. Áreas en que se realiza la gestión de riesgo

Falta de planificación de TI y no existencia de indicadores y métricas de TI. Al consultar a las empresas sobre el problema de TI más frecuente que se ha experimentado en los últimos 12 meses, un 60,7% de las empresas nos expresó que es la inexistencia de indicadores de eficiencia de TI y el segundo problema más frecuente es la falta de procesos de revisión y evaluación de los indicadores y objetivos de TI. El 40% de las organizaciones no miden la aportación de TI al negocio y el 13 % no planifica a TI.

Falta de formación de personal en Gobernanza de TI. No hay técnicos formados y especializados en gobernanza de TI que puedan asesorar a las organizaciones para lograr una mejor gobernanza. Un 40% de las organizaciones consideran que se carece de información sobre las soluciones y que se carece de recursos expertos para la implementación de esas prácticas tal como se muestra en la figura 9.

Bajo presupuesto de TI o falta de presupuesto de TI. En general no se corresponde la importancia que los empresarios le asignan a TI como elemento que permite la consecución de una estrategia (63% la considera imprescindible (figura 4) en relación a los gastos del presupuesto asignados a TI (47% le asigna entre un 5 y un 10% (Tabla 1)) y en muchos casos no existe un presupuesto para TI. Esto dificulta el contar con una infraestructura de TI y recursos que apoyen los objetivos del negocio en la organización.

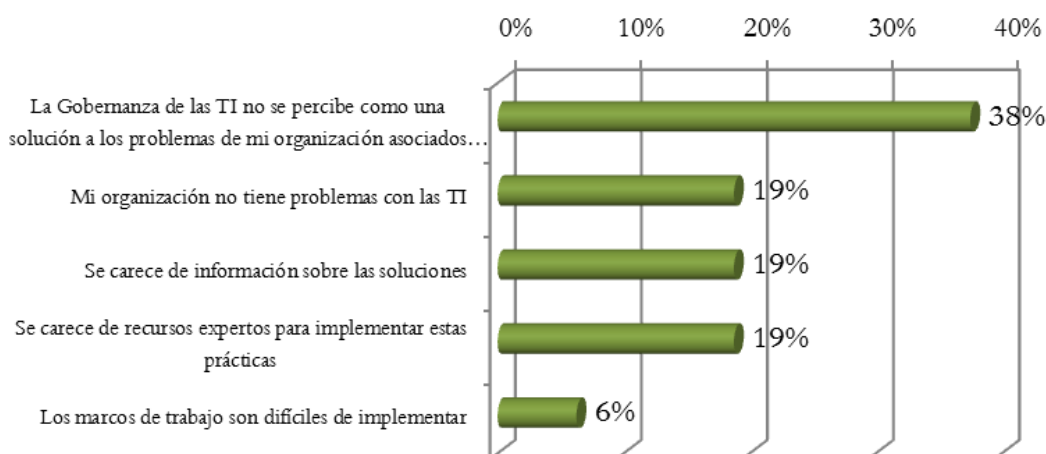


Figura 9. Motivos de no implementación de practicas

Problemas económicos, financieros, de tamaño e infraestructura. El contar con los recursos económicos apropiados para poder asignar un presupuesto que permita tener un tamaño e infraestructura que posibilite el alineamiento estratégico de TI con los objetivos del negocio es importante para poder lograr una buena gobernanza de TI. Un 6,4 % de las organizaciones consultadas expresaron como obstáculo para aplicar buenas prácticas de gobernanza el tamaño de la organización y la falta de infraestructura y un 3,2 % considero como obstáculo la centralización de los servicios (figura 7).

Solo un 34 % de las organizaciones consultadas utilizan estas técnicas para la aprobación de los proyectos a través de un análisis de viabilidad con un análisis económico y cualitativo, que incluya la identificación de los riesgos y las alternativas para alinearse con los objetivos del negocio. Observamos según el estudio de análisis de madurez de TI en PyMEs del Uruguay que las organizaciones con mayor nivel de madurez cuentan con una infraestructura de TI definida y adecuada tanto en estructura física y lógica como en recursos humanos.

9. Conclusiones

A través del estudio de campo presentado anteriormente y del análisis de los resultados obtenidos se observa que la incorporación de buenas prácticas de inversión mínima y de inversión mediana puede mejorar sustantivamente la gestión del gobierno de TI en el contexto de las pequeñas y medianas empresas.

A continuación se analizan las buenas prácticas recomendadas que requieren una inversión mínima por parte de la organización y se presenta una tabla con la incidencia de cada una de ellas en la mejora de la gobernanza de TI (Tabla 2).

Buenas prácticas que requieren un nivel mínimo de inversión:

- Toma de decisiones conjunta: mejoraría la gobernanza en el 67% de las organizaciones (según figuras 1 y 2).
- Mejorar la gestión de riesgos y seguridad: mejoraría la gobernanza en el 70% de las organizaciones (según figura 5 y 11).

Reducir la falta de conocimiento de buenas prácticas de TI: mejoraría la gobernanza en el 90% de las organizaciones (según figuras 6, 7 y 12).

- Mejorar la formación de personal en Gobernanza de TI: mejoraría la gobernanza en el 40% de las organizaciones (según figura 7).
- Mejorar la cultura organizacional: mejoraría la gobernanza en el 40% de las organizaciones (según figura 7 y 12).
- Mejorar la planificación de TI y no existencia de indicadores y métricas de TI: mejoraría la gobernanza en un 73 % de las organizaciones (según figura 7).

Tabla 2. Porcentajes de incidencia de cada práctica de inversión mínima para lograr una mejor gobernanza de TI.

Buenas prácticas de inversión mínima	% de incidencia en la mejora de los problemas más comunes.
Toma de decisiones conjunta	67%
Mejorar la gestión de riesgos y seguridad	70%
Mejorar la falta de conocimiento de buenas prácticas de TI	90%
Mejorar la formación de personal en Gobernanza de TI	40%
Mejorar la cultura organizacional	40%
Mejorar la planificación de TI y no existencia de indicadores y métricas de TI	73 %

A continuación se analizan las buenas prácticas recomendadas que requieren una inversión más importante por parte de la organización y se presenta una tabla con la incidencia de cada una en la mejora de la gobernanza de TI (Tabla 3).

Buenas prácticas que requieren una inversión más importante:

- Asignar un presupuesto o mejorar el presupuesto de TI - Mejoraría la gobernanza en un 23 % de las organizaciones (según figura 7).
- Mejorar condiciones económicas de tamaño e infraestructura – Mejoraría la gobernanza en un 6.4 % de las organizaciones (según figura 7).

Tabla 3. Porcentajes de incidencia de cada práctica de inversión más importante para lograr una mejor gobernanza de TI.

Buenas prácticas que requieren una inversión más importante	% de incidencia en la mejora de los problemas más comunes.
Asignar un presupuesto o mejorar el presupuesto de TI	23 %
Mejorar condiciones económicas de tamaño e infraestructura	6,4%

Podemos apreciar que el **impacto de mejora** en la gobernanza de TI al aplicar buenas prácticas con un nivel de inversión mínimo es **muy importante** (entre un 40 y un 90%), mientras que es **importante** (entre un 6,4 y un 23%) al aplicar buenas prácticas que requieren una inversión mediana.

Referencias

- [1] A.J. Arroyo, J.D. Carrillo, The status of IT Governance in Spanish organizations. Analysis and conclusions for identifying best practices, in, 2009.
- [2] BCU, Instituciones de intermediación financiera - Normativa sobre gobierno corporativo y sistema de gestión integral de riesgos., in, 2008.
- [3] M. Bunge, La Ciencia Su Método Y Su Filosofía, Eudeba, Buenos Aires, 1960.
- [4] A. Calder, The IT Governance Toolkit-v05, in, IT Governance Publishing, 2008.
- [5] DINAPYME, Criterio de clasificación de Empresas en el Uruguay, in, 1995.
- [6] DINAPYME, Estructura de las Empresas PYMES en el Uruguay, in: MIEM (Ed.) Observatorio PYME Uruguay, 2005.
- [7] U. DINAPYME, Teresa Herrera & Asociados Consultoría, Encuesta Nacional de mPymes industriales y de servicios, (2008).
- [8] ESADE, Corporate Governance, el buen gobierno de la empresa, in: EGuíame!, la Caixa, 2004.
- [9] Fundatec, Análisis sectorial de implantación de las TIC en la pyme española, in: I.P. 2008 (Ed.), 2008.
- [10] ISO, ISO/IEC 38500:2008. Corporate Governance for Information Technology., in, ISO, 2008.
- [11] ITGI, CobiT© 4.1, in, ISACA, USA, 2007.
- [12] ITGI, Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, in, ISACA, USA, 2008.
- [13] ITGI, Marco de riesgos de TI. Risk IT, in, ISACA, 2009.
- [14] ITGI, COBIT® 5 Design Paper Exposure Draft, in, ISACA, 2010.
- [15] N. Malhotra, Investigación de mercado, Prentice-Hall, Georgia, 2004.
- [16] OCDE, Principios de Gobierno Corporativo de la OCDE, in, Organización para la cooperación y el desarrollo económicos, París, 2004.
- [17] E.B. Sánchez, La investigación científica: Teoría y metodología, in, Zacatecas, 2003.
- [18] C. Scaronne, La informalidad en las MIPYMES de Uruguay. Análisis de los costos de la formalidad, Ministerio de Industria, Energía y Minería, Montevideo, Uruguay, 2007.
- [19] C. Symons, IT Governance Framework. Structures, Processes, And Communication, in: C.S.-. Forrester (Ed.), 2005.
- [20] I. Terán, Inversión en TI: Un partner cada vez más importante para la PYME Latinoamericana, in: InfoWeek, 2009.

[21] W. Van_Grembergen, S. De_Haes, An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment, *Information Systems Management*, 26 (2007) 123-137.

[22] P. Weill, J. Ross, *IT Governance. How top performers manage IT decision rights for superior results*, in, Harvard Business School Press, Boston, Massachusetts, 2004.

[23] P. Weill, J. Ross, Four Questions Every CEO Should Ask About IT, in: *The Wall Street Journal*, 2011.

ANEXO II - Knowledge Management Steps, Tools, Techniques and Influencing Factors in SMEs

Systematic Literature Review

Helena GarbarinoAlberti
Garbarino@ort.edu.uy
Facultad de Ingeniería
Universidad ORT Uruguay
Montevideo, Uruguay

Sebastián Ayala Pastorino
Ayala@ort.edu.uy
Facultad de Ingeniería
Universidad ORT Uruguay
Montevideo, Uruguay

Abstract

Knowledge management is becoming increasingly important in creating value and sustainable competitive advantage in organization. Achieving an efficient knowledge management depends on how its different phases are implemented as well as certain critical success factors. Because of this, the purpose of this article is to report a systematic mapping of the literature to identify, extract and categorize existing research on the stages or phases, tools, techniques and factors influencing knowledge management in SMEs.

The process for mapping and existing items, steps, tools, techniques, types of factors reported and the research methods used to identify them are identified is described. These results will be used as a basis for further empirical study on Knowledge Management in the SME sector Uruguay

Palabras claves

Sistematic literature review, Knowledge management ,Strategy, PyMES, Success Factors, Obstacles, Barriers, Tools, Techniques.

I. INTRODUCCIÓN

Se puede definir la gestión del conocimiento (de aquí en más GC) como la colección de procesos que gobiernan la creación, diseminación, y utilización del conocimiento [1]. La GC implica cualquier proceso o práctica para crear, adquirir, capturar, compartir y usar conocimiento, cualquiera sea el lugar donde resida, para mejorar el aprendizaje y el desempeño en las organizaciones [2].

Las Pequeñas y Medianas Empresas (de aquí en más PyMEs) son muy importantes en las distintas economías del mundo. Estadísticas de la SBA (U.S. Small Business Administration) de Estados Unidos muestran que las pequeñas empresas generan alrededor del 50% de todas las ventas estadounidenses, y contribuyen al 50 % del PBI privado. Además, emplean a más del 50% de la fuerza laboral de ese país [3]. En el Uruguay, estas empresas aportan el 33% de PBI y el 25% de la inversión [3]. Se considera como pequeña empresa a las de hasta 19 trabajadores y mediana empresa a las que poseen entre 20 y 99. Esta clasificación varía según el país que se considere, siendo en general mayores los límites de cada intervalo a mayor tamaño del país y volumen económico.

II. MAPEO SISTEMÁTICO DE LITERATURA

De acuerdo con Kitchenham [6] y en base a los lineamientos provistos en [7] y en [8], los pasos seguidos para el mapeo sistemático son:

- A. Definición de las preguntas de investigación.
- B. Búsqueda de la literatura relevante.
- C. Selección de los estudios pertinentes.
- D. Clasificación de los artículos.
- E. Extracción y agregación de los datos.

Típicamente, las PyMEs presentan una estructura organizacional plana, informal y flexible con una supervisión directa [4] en la que un responsable, director general, cumple múltiples funciones, es el responsable principal en la toma de decisiones y asume todos los riesgos. Esta particularidad hace que sea altamente relevante utilizar elementos de GC para gestionar la creación, adquisición, captura y diseminación del conocimiento de forma eficiente como factor clave para el logro de los objetivos organizacionales.

En la literatura relativa a GC en las organizaciones existe una serie de trabajos orientados a identificar sus procesos, las fases que posibilitan la creación del conocimiento así como los factores de éxito, obstáculos y barreras que inciden en su implementación. En este contexto, se entiende por factores de éxito a los elementos organizacionales que facilitan y contribuyen de manera positiva a una iniciativa de implementación de GC. El conocerlos permitirá poder analizar el nivel en el que se encuentra la organización en relación a la GC y tomar acciones estratégicas de mejora a través de la implementación de procesos y buenas prácticas, favoreciendo de esta manera la mejora continua y el logro de los objetivos del negocio.

El propósito de este artículo es reportar los resultados de un mapeo sistemático de la literatura cuyo objetivo fue identificar y conocer cuáles son, en efecto, las etapas, herramientas, técnicas, y factores críticos de éxito de la GC en las organizaciones PyMEs que inciden en una iniciativa de mejora de GC reportado en la literatura identificada en el mapeo sistemático.

El resto del artículo está organizado de la siguiente manera. En la sección 2 se describe el proceso seguido para el mapeo sistemático y se presentan los resultados obtenidos. En la sección 3 se presenta las etapas, herramientas, técnicas y factores extraídos del análisis de la literatura. Finalmente, en la sección 4 se presentan las conclusiones del estudio y se mencionan los trabajos futuros.

A. Preguntas de Investigación

Para este estudio, las preguntas que se buscan responder son las siguientes:

- 1.- ¿Cuáles son los estudios existentes acerca de las etapas, herramientas, técnicas y factores críticos de éxito que inciden en la GC en las PyMEs?
- 2.- ¿Qué clases de fases, herramientas, técnicas y factores han sido identificados en cada estudio?

B. Búsqueda de la Literatura Relevante

La identificación de la literatura relevante al tema implica definir, primeramente, las cadenas de búsqueda a utilizar en las bases de datos bibliográficas. Para la construcción de estas cadenas se utilizaron las siguientes palabras claves: “knowledge management”, “KM”, “SMES”, “success”, “failure”, “obstacles”, “barriers”, “stages”, “tools” y “technics”.

Para las búsquedas se utilizaron las siguientes bases de datos bibliográficas: SpringerLink (www.springerlink.com), ScienceDirect (www.sciencedirect.com), IEEExplore (ieeexplore.ieee.org) y ACM Digital Library (portal.acm.org).

Se optó por utilizar cadenas cortas de la forma <cadena1> AND <cadena2> AND <cadena3>, donde <cadena1> contiene en forma alternada las expresiones “knowledge management” y “KM” y <cadena2> varía sucesivamente con las expresiones “success”, “failure”, “obstacles”, “stages”, “tools” y “technics” mientras que <cadena3> contiene la expresión “SMES”.

De este modo, se ejecutaron 48 búsquedas en la base de datos. Las búsquedas se realizaron sobre los campos “Titulo”, “Resumen” y “Palabras claves”, y los resultados se presentan en la Tabla 1.

TABLA 1. CANTIDADES Y PORCENTAJES DE ARTÍCULOS ENCONTRADOS EN LAS BÚSQUEDAS.

Cadena 1	Cadena 2	Cadena 3	SpringerLink	ScienceDirect	IEEExplore	ACM	Porcentaje
“knowledge management”	success	SMES	12	15	10	9	46
	failure		4	6	2	3	15
“KM”	obstacles		3	5	4	5	17
	stages		10	14	12	13	49
	tools		7	9	8	10	34
	technics		8	11	10	10	39
TOTAL			44	60	46	50	200

C. Selección de los artículos pertinentes.

Los criterios de inclusión/exclusión definidos para este estudio son:

- **Inclusión:** artículos de revistas y de anales o actas de conferencia, capítulos de libros, reportes técnicos y literatura gris publicados en cualquier fecha que presenten resultados de estudios empíricos.
- **Exclusión:** artículos en los que la sigla KM no signifique “knowledge management” o que la sigla SMES no signifique “small and medium enterprises”. Artículos publicados en revistas o actas de conferencias no arbitradas.

La selección se realizó en base a la lectura del título, del resumen y de las palabras claves de cada artículo obtenido en las búsquedas, aplicando los criterios de selección precedentes.

La Tabla 2 presenta a continuación los 32 artículos y el porcentaje de los mismos que cumplen con los criterios definidos:

TABLA 2. CANTIDADES DE ARTÍCULOS ENCONTRADOS QUE CUMPLEN CON LOS CRITERIOS DEFINIDOS.

Cadena 1	Cadena 2	Cadena 3	Cantidad de Artículos - %
“Knowledge management” “KM”	Success	SMES	7 - 21,88
	Failure		1 - 3,13
	Obstacles		2 - 6,25
	Stages		10 - 31,25
	Tools		5 - 15,63
			7 - 21,88
	Technics		
TOTAL			32 - 100

La literatura identificada y analizada que cumple con los criterios definidos esta discriminada de la siguiente manera: 19 Artículos de revistas, 2 Actas de conferencias, 5 Reportes técnicos, 4 Capítulos de libros, 1 Tesis de maestría y 1 Tesis de doctorado y se presentan a continuación en la Tabla 3:

TABLA 3. TIPO DE PUBLICACIONES ENCONTRADAS QUE CUMPLEN CRITERIOS.

Tipo de Publicación	Cantidad de Artículos
Artículos de revista	19
Reportes técnicos	5
Capítulos de libros	4
Actas de conferencias	2
Tesis de maestría	1
Tesis de doctorado	1
TOTAL	32

D. Clasificación de los artículos

Para responder las preguntas de investigación formuladas al comienzo es necesario establecer qué datos deben extraerse de cada artículo seleccionado en el paso anterior.

La clasificación de los artículos se hizo en base a las siguientes categorías:

- 1) Medios de publicación.
- 2) Año de publicación.
- 3) Tipos de fases reportadas.
- 4) Tipos de herramientas reportadas.
- 5) Tipos de técnicas reportadas.
- 6) Tipos de factores reportados.
- 7) Tipos de estudios realizados.
- 8) Nombres de los autores relevantes.
- 9) Nombres de las revistas, conferencias, publicaciones e instituciones.

E. Extracción y agregación de datos.

La extracción de datos de los estudios seleccionados se realizó en forma independiente por cada autor a través de la lectura de cada artículo en forma completa al tiempo que se completaba una planilla de extracción de datos con el registro de los datos mencionados en la sub-sección anterior. Una vez procesados todos los artículos se hizo una puesta en común para verificar las coincidencias y también para identificar y resolver las discrepancias que pudieran haberse encontrado.

Como resultado de este proceso, la Tabla 4 y la Tabla 5, ordenadas por año de publicación, presentan un extracto de los datos recopilados de cada artículo.

TABLA 4. LISTA DE ESTUDIOS INCLUIDOS EN EL MAPEO

Ref.	Año	Medio de publicación	Tipo de fase	Tipo de herramienta
[17]	1995	Cap.de libro	Socialización, Externalización, Internalización Combinación.	
[13]	1995	Revista	Socialización, Externalización, Internalización Combinación.	Comunidades de práctica y Grupos expertos
[11]	1997	Cap.de libro		
[18]	1998	Revista	Generación, Codificación, Transferencia.	Mapas, Patentes, Redes, Fusión o Adquisición de Conocimiento
[12]	1998	Revista	Generación, Codificación, Transferencia.	

[15]	1999	Cap.de libro	Socialización, Externalización, Internalización Combinación.	Comunidades de Práctica y Grupos Expertos.
[21]	2000	Conferencia		Memoria organizacional
[16]	2001	Cap.de libro	Identificación Adquisición Desarrollo Compartir o Distribuir Uso Retención	Mapas y Benchmarking, Fusión o Adquisición de conocimiento. Lecciones aprendidas y Grupos Expertos. Comunidades de práctica. Redes. Mejores prácticas. Análisis de redes Sociales. Accesibilidad y Diseño del área de trabajo. Memoria organizacional.
[1]	2001	Tesis Doctoral	Generación Codificación Transferencia Uso Retención	Accesibilidad y Diseño del área de trabajo. Mapas. Patentes, Memoria organizacional.
[14]	2002	Revista		
[25]	2002	Conferencia	Retención	Memoria Organizacional
[26]	2002	Revista	Compartir o Distribuir	Comunidades de práctica
[37]	2004	Conferencia		
[38]	2005	Conferencia		
[20]	2006	Conferencia		
[2]	2007	Capítulo de Libro	Generación Codificación Transferencia	Redes, Fusión o Adquisición de conocimientos. Mapas, Patentes
[24]	2008	Conferencia		
[27]	2008	Conferencia		
[28]	2009	Conferencia		
[30]	2009	Conferencia		
[31]	2009	Conferencia		
[19]	2010	Conferencia		
[22]	2010	Conferencia		
[23]	2010	Conferencia		
[29]	2010	Conferencia		

[32]	2010	Conferencia		
[39]	2010	Conferencia		
[35]	2011	Conferencia		
[36]	2011	Conferencia		
[34]	2012	Conferencia		
[33]	2013	Conferencia		
[40]	2014	Conferencia		

TABLA 5. LISTA DE ESTUDIOS INCLUIDOS EN EL MAPEO. CONTINUACIÓN

Ref.	Año	Tipos de Técnica	Tipo de factores	Tipo de estudio
[17]	1995	Cámaras web Videoconferencias Realidad virtual	Éxito, Obstáculos	Encuesta, Reporte de exp.
[13]	1995	Cámaras web Videoconferencias Realidad virtual	Éxito, Obstáculos, Innovadores	Encuesta, Entrevista
[11]	1997		Éxito, Obstáculos	Cuestionario, Caso de Estudio
[18]	1998	Sistemas expertos	Éxito, Fracaso	Entrevista
[12]	1998	Charlas informales, Contacto personal y Mentoring	Éxito	Encuesta, Entrevista
[15]	1999	Cámaras web Videoconferencias y Realidad virtual. Bases de conocimiento y E- learning. Clasificación y Clustering.	Éxito, Fracaso, Obstáculos	Reporte de exp.
[21]	2000		Éxito, Fracaso, Obstáculos	Caso de Estudio
[1]	2001	Sistemas expertos	Éxito, Obstáculos, Fracaso.	Entrevista

[16]	2001		Éxito, Fracaso	Reporte de exp. Encuesta
[14]	2002		Éxito	Caso de Estudio
[25]	2002		Éxito, Fracaso	Encuesta
[26]	2002		Éxito	Entrevista
[37]	2004			
[38]	2005		Obstáculos	Encuesta
[20]	2006		Éxito, Fracaso	Encuesta
[2]	2007	Sistemas expertos. Charlas informales. Contacto personal y Mentoring	Éxito, Obstáculos, Fracaso.	Reporte de experiencia, Encuesta
[24]	2008		Éxito, Fracaso	Caso de Estudio
[27]	2008		Éxito, Obstáculos	Caso de Estudio
[28]	2009		Éxito, Fracaso	Reporte de Experiencia
[30]	2009		Éxito	Caso de Estudio
[31]	2009		Éxito, Fracaso	Caso de Estudio
[19]	2010			Caso de Estudio
[22]	2010		Éxito, Fracaso	Entrevista
[23]	2010			Encuesta
[29]	2010		Éxito	Caso de Estudio
[32]	2010		Éxito, Fracaso	Caso de Estudio
[39]	2010			Caso de Estudio
[35]	2011			Encuesta
[36]	2011			Caso de Estudio
[34]	2012			Caso de Estudio

[33]	2013			Encuesta
[40]	2014		Éxito	Caso de Estudio

Los datos de la Tabla 4 y de la Tabla 5 permiten responder en forma directa las preguntas de investigación formuladas al comienzo.

Pregunta 1: ¿Cuáles son los estudios existentes acerca de las etapas, herramientas y factores críticos de éxito que inciden en la GC en las PyMEs?

La columna “Ref.” de la Tabla 4 y de la Tabla 5 contiene las referencias bibliográficas de los 32 estudios considerados para este trabajo, ordenados por año de publicación. Los datos bibliográficos completos se encuentran en la sección Referencias al final del artículo.

Pregunta 2: ¿Qué clases de fases, herramientas, técnicas y factores han sido identificados en cada estudio?

La columna “Tipo de Fase” de la Tabla 4 contiene los tipos de fases analizadas o identificadas en el respectivo artículo. Tres de los estudios seleccionados se refieren a un tipo de clasificación de las fases de GC (Socialización, Externalización, Internalización, Combinación), tres estudios a otro tipo de clasificación de fases de GC (Generación, Codificación, Transferencia), tres estudios a un tercer tipo de clasificación de GC (Identificación, Adquisición, Desarrollo, Compartir o Distribuir, Uso, Retención), mientras que uno de los estudios se refiere a una combinación de la clasificación de fases definidas por Davempont y Probst (Generación, Codificación, Transferencia, Uso, Retención). La Tabla 12 presenta las etapas, cantidad de menciones y el porcentaje de menciones ordenado de mayor a menor para mostrar la relevancia de las mismas en la literatura.

La columna “Tipo de Herramienta” de la Tabla 4 contiene los tipos de herramientas analizadas o identificadas en el respectivo artículo. Diez de los estudios seleccionados se refieren al uso de herramientas para la GC. La Tabla 14 presenta las Herramientas, cantidad de menciones y el porcentaje de menciones ordenado de mayor a menor para mostrar la relevancia de las mismas en la literatura.

La columna “Tipo de Herramienta” de la Tabla 4 contiene los tipos de herramientas analizadas o identificadas en el respectivo artículo. Diez de los estudios seleccionados se refieren al uso de herramientas para la GC. La Tabla 14 presenta las Herramientas, cantidad de menciones y el porcentaje de menciones ordenado de mayor a menor para mostrar la relevancia de las mismas en la literatura.

La columna “Tipo de Técnica” de la Tabla 5 contiene los tipos de técnicas analizadas o identificadas en el respectivo artículo. Diez de los estudios seleccionados se refieren al uso de técnicas para la GC. La Tabla 15 presenta las Herramientas, cantidad de menciones y el porcentaje de menciones ordenado de mayor a menor para mostrar la relevancia de las mismas en la literatura.

La columna “Tipo de Factores” de la Tabla 5 contiene los tipos de factores analizados o identificados en el respectivo artículo. Se cuentan 24 artículos que refieren a factores de éxito, fracaso u obstáculos. De estos, 23 se centraron en la identificación de factores de éxito que afectan positivamente a la GC, 9 a los factores que obstaculizan a la GC y 13 en la identificación de factores de éxito, fracaso u obstáculos a la gestión del conocimiento. La Tabla 19 presenta los tipos de factores, cantidad de menciones y el porcentaje de menciones ordenado de mayor a menor para mostrar la relevancia de los mismos en la literatura.

La columna “Tipo de Estudio” de la Tabla 5 contiene las técnicas o combinaciones de técnicas de investigación utilizadas en el respectivo artículo, manteniendo las denominaciones dadas por los autores de cada artículo. Se identifican cinco tipos de estudio (Encuesta, Reporte de experiencia, Entrevista, Caso de estudio y Cuestionario). La Tabla 6 presenta las cantidades y porcentajes de utilización de estas técnicas en los estudios considerados.

TABLA 6. TIPOS DE ESTUDIOS REALIZADOS.

Tipos de Estudio	Cantidad Art.	%
Encuesta	11	29,73
Reporte de experiencia	5	13,51
Entrevista	6	16,22
Caso de Estudio	14	37,84
Cuestionario	1	2,7
TOTALES	37	100

La columna “Año” de la Tabla 4 y de la Tabla 5 contiene el año de publicación de cada estudio.

La Tabla 7 presenta de manera agregada, la cantidad de estudios publicados por año, desde 1995 hasta marzo del 2014.

TABLA 7. ESTUDIOS PUBLICADOS POR AÑO

Año	Cantidad	%
Año 1995	2	6,25
Año 1997	1	3,13
Año 1998	2	6,25
Año 1999	1	3,13
Año 2000	1	3,13
Año 2001	2	6,25
Año 2002	3	9,38
Año 2004	1	3,13
Año 2005	1	3,13
Año 2006	1	3,13
Año 2007	1	3,13
Año 2008	2	6,25
Año 2009	3	9,38
Año 2010	6	18,75
Año 2011	2	6,25

Año 2012	1	3,13
Año 2013	1	3,13
Año 2014	1	3,13
TOTALES	32	100,00

En el total de estudios considerados para este trabajo, hay tres autores que se destacan por tener dos o más artículos publicados, según se muestra en la Tabla 8.

TABLA 8. PRINCIPALES INVESTIGADORES EN EL TEMA.

Investigador	Cantidad Art.	%
I. Nonaka and H. Takeuchi	3	42,86
T. Davenport	2	28,57
Probst	2	28,57
TOTALES	7	100,00

Como se puede apreciar en la Tabla 9, las principales publicaciones son las conferencias, las revistas (journals) y los libros. De los 32 estudios considerados, 19 (73,08 %) son conferencias, 5 (19,23 %) son journals y 2 (7,69 %) libros.

TABLA 9. PRINCIPALES TIPOS DE PUBLICACIONES SOBRE EL TEMA.

Tipo	Cantidad	%
Conferencias (Conference)	19	73,08
Revistas (Journals)	5	19,23
Libros (Book)	2	7,69
TOTALES	26	100,00

De los 32 estudios considerados, dos revistas y una conferencia concentran más de la mitad de los trabajos publicados sobre el tema, 24 (75%), y dentro de las conferencias y journals publicados sobre el tema, la IEEE Conference P. es la que más publicaciones tiene (73,08%), seguida por la Oxford University P. Journal (11,54%) y luego por la Harvard Business School P. Journal, según se muestra a continuación, en la Tabla 10:

TABLA 10. PRINCIPALES REVISTAS (JOURNALS) Y CONFERENCIAS.

Nombre	Tipo	Cantidad	%
IEEE CONFERENCES	Conference	19	79,16
Oxford University	Journals	3	12,5
Harvard Business School	Journals	2	8,33
TOTALES		24	100,00

III. CATEGORIZACIÓN DE ETAPAS, FACTORES CRÍTICOS DE ÉXITO, HERRAMIENTAS Y TÉCNICAS IDENTIFICADAS

Con la finalidad de conocer cuáles son las etapas, herramientas, técnicas y factores críticos de éxito de la GC reportados en la literatura identificada en el mapeo sistemático, se fue registrando en una planilla las palabras o frases que cada autor utilizó para referenciarlos. Los resultados obtenidos se sintetizan en la Tabla 11.

TABLA 11. ETAPAS Y AUTORES QUE LAS DEFINEN, SIGNIFICADO DE LAS MISMAS Y CANTIDAD DE MENCIONES EN LA LITERATURA

Autor	Etapa	Significado	Cantidad Menciones - %
I. Nonaka and H. Takeuchi	Socialización	Implica la conversión del conocimiento tácito en conocimiento tácito.	3 - 9,38
	Externalización	Implica la conversión del conocimiento tácito en conocimiento explícito.	3 - 9,38
	Internalización	Implica la conversión del conocimiento explícito en conocimiento tácito.	3 - 9,38
	Combinación	Implica la conversión del conocimiento explícito en conocimiento explícito.	3 - 9,38
Davenport	Generación	Implica actividades para incrementar el stock del conocimiento.	4 - 12,50
	Codificación	Implica poner el conocimiento disponible de forma que sea accesible a quienes lo necesitan.	4 - 12,50
	Transferencia	Implica transmitir el conocimiento.	4 - 12,50
Probst	Identificación	Implica determinar dónde está el conocimiento. Que es lo que falta conocer.	1 - 3,13
	Adquisición	Implica adquirir el faltante de conocimiento.	1 - 3,13
	Desarrollo	Implica desarrollar nuevas habilidades, productos e ideas	1 - 3,13
	Compartir o Distribuir el conocimiento	Implica intercambiar el conocimiento disponible a quien lo requiera	2 - 6,25
	Retención del Conocimiento	Implica el almacenamiento y actualización del conocimiento.	3- 9,38
	Uso	Implica la utilización del conocimiento por quien lo requiera	2 - 6,25

A partir del análisis de la información presentada anteriormente en la Tabla 11, se puede apreciar que existen 3 clasificaciones de etapas o fases de GC definidas por cuatro autores. Dos de ellos, Nonaka y Takeuchi, plantean la existencia de cuatro fases a las que le llaman Socialización, Externalización, Internalización y Combinación, a través de las cuales se crea y convierte el conocimiento cíclicamente en forma de espiral.

Davenport por su parte define tres etapas a las que denomina Generación, Codificación y Transferencia, mientras que Probst plantea la existencia de seis etapas a las que llama Identificación, Adquisición, Desarrollo, Compartir o Distribuir el conocimiento, Uso y Retención del conocimiento.

Existen algunas similitudes en las características de las etapas definidas por los autores como podemos apreciar en sus definiciones en la Tabla 11, como es el caso de la etapa de transferencia de Davenport y la de Compartir o Distribuir el conocimiento de Probst, donde claramente hacen mención al mismo concepto.

Conocer las etapas de Gestión de Conocimiento es de suma importancia para las organizaciones ya que favorece la mejora de esta gestión y el logro de los objetivos del negocio.

En relación a las herramientas de Gestión de Conocimiento, la Tabla 12 muestra a continuación las identificadas en la literatura, sus definiciones según los autores que las mencionan, la cantidad de veces que son mencionadas y el porcentaje de menciones de las mismas.

TABLA 12. HERRAMIENTAS IDENTIFICADAS, SUS DEFINICIONES SEGÚN LOS AUTORES QUE LAS MENCIONAN, LA CANTIDAD DE VECES QUE SON MENCIONADAS Y EL PORCENTAJE DE MENCIONES DE LAS MISMAS

Herramientas	Definición	Autores	Cantidad Menciones-%
Accesibilidad	Implica que el conocimiento esté disponible para quien lo necesite.	[1] L. Paradela, [16] R. Bergmann	2 - 6,25
Diseño del área de trabajo	Implica definir y organizar el lugar de trabajo de forma que favorezca el intercambio de conocimientos entre los integrantes del mismo.	[1] L. Paradela, [16] R. Bergmann	2 - 6,25
Memoria organizacional	Es la representación de los conocimientos de una organización en forma explícita y persistente.	[1] L. Paradela, [16] R. Bergmann, [21]R.Crossand,L.Baird,[25] M. Jennex, Olfman	4 - 12,50
Mapas	Consiste en una forma de representación del conocimiento para que pueda ser consultado y utilizado por quien lo necesite.	[1] L. Paradela, [2] A. Del Moral, J.Pazos, E.Rodriguez, S.Suarez [16] R. Bergmann, [18] T. Davenport	4 - 12,50
Patentes	Implica el registro del conocimiento necesario para	[1] L. Paradela, [2] A. Del Moral, J.Pazos, E.Rodriguez,, S.Suarez,	3 - 9,38

	determinado producto o servicio.	[[8] Arksey, H, L. O'Malley	
Benchmarking	Implica determinar dónde estamos y adonde queremos llegar. Proceso de determinar quién es el mejor, quien establece estándares, cuales son los estándares. Es determinar que hay detrás de los números.	[16] R. Bergmann	1 - 3,13
Fusión o adquisición de conocimiento	Implica asociarse o comprar conocimiento para generar de este en la organización.	[2] A. Del Moral, J.Pazos, E.Rodriguez,, S.Suarez, [16] R. Bergmann, [18] T. Davenport	3 - 9,38
Lecciones aprendidas	Implica el registro de lo aprendido para su uso posterior.	[16] R. Bergmann	1 - 3,13
Grupos expertos	Implica un grupo de personas especialistas en determinada área que aportan conocimiento a la organización.	[13],[15] I. Nonaka, H. Takeuchi, [16] R. Bergmann	3 - 9,38
Comunidades de práctica	Grupos de personas que comparten un interés, conjunto de problemas o pasión por un tema y que profundizan sus conocimientos interactuando de manera habitual.	[13],[15] I. Nonaka, H. Takeuchi, [16] R. Bergmann, [26] E. Wegner, Mc Dermott, R.Snyder	4 - 12,50
Redes	Implica grupos de personas con determinados roles o intereses comunes que comparten conocimiento.	[2] A.Del Moral, J.Pazos, E.Rodriguez, S.Suarez, [16] R. Bergmann, [18] T. Davenport	3 - 9,38
Mejores prácticas	Implica registrar las mejores formas de realizar una tarea para que la pueda consultar quien las necesite.	[16] R. Bergmann	1 - 3,13
Análisis de redes	Implica la	[16] R. Bergmann	1 - 3,13

Sociales	utilización de las redes sociales como forma de compartir e intercambiar conocimiento.		
----------	--	--	--

En relación a las técnicas de GC, la Tabla 13 muestra a continuación las identificadas en la literatura, sus definiciones según los autores que las mencionan y la cantidad de veces que son mencionadas, mientras que la tabla 14 presenta la cantidad y el porcentaje de menciones de las mismas:

TABLA 13. TÉCNICAS, DEFINICIÓN, AUTORES Y CANTIDAD DE VECES.

Técnicas	Definición	Autores	Cantidad de veces
Cámara web	Implica la utilización de la imagen como forma de generar y compartir conocimiento.	[13],[15], [17] I. Nonaka, H. Takeuchi	3
Videoconferencia	Implica la utilización del video, imagen y sonido como forma de generar y compartir conocimiento.	[13],[15], [17] I. Nonaka, H. Takeuchi	3
Realidad virtual	Implica la simulación de una situación de la realidad como forma de generar y compartir conocimiento.	[13],[15], [17] I. Nonaka, H. Takeuchi	3
Sistema expertos	Implica la utilización de sistemas especializados en determinada área del conocimiento.	[1] L. Paradela, [2] A.Del Moral, J.Pazos, E.Rodriguez,, S.Suarez, [18] T.	3
Charla informales	Implica compartir experiencia y conocimiento entre distintos miembros en la organización de manera no planificada.	[2] A.Del Moral, J.Pazos, E.Rodriguez,, S.Suarez, [12] T. Davenport, L. Brusak	3

Coaching	Implica la consulta y asesoramiento con una persona que pueda aportar de su conocimiento.	[2] A.Del Moral, J.Pazos, E.Rodriguez,, S.Suarez, [12] T. Davenport, L.	2
Mentoring	Implica el crecimiento personal de una persona de forma abarcativa y general a través de un mentor, quien aconseja y enseña gradualmente en base a su experiencia.	[2] A.Del Moral, J.Pazos, E.Rodriguez,, S.Suarez, [12] T. Davenport, L. Prusak	2
Bases del Conocimiento	Implica bases de datos que contienen conocimiento para ser utilizado por quien lo necesite.	[15] I. Nonaka, H. Takeuchi	1
E-learning	Implica una forma electrónica de aprendizaje para lograr adquirir un determinado conocimiento.	[15] I. Nonaka, H. Takeuchi	1
Clasificación	Implica ordenar el conocimiento de forma que sea de más fácil acceso para quien lo requiera.	[15] I. Nonaka, H. Takeuchi	1
Clustering	Implica agrupar el conocimiento en determinados grupos de interés, roles, o algún criterio para que sea de fácil acceso a quien lo necesite y lo deba tener.	[15] I. Nonaka, H. Takeuchi	1

TABLA 14. TIPO DE TÉCNICAS, CANTIDAD Y PORCENTAJES DE MENCIONES

Tipo de Técnicas	Cantidad de menciones	%
Cámara web	3	13,04
Videoconferencia	3	13,04

Realidad Virtual	3	13,04
Sistemas Expertos	3	13,04
Charla Informales	3	13,04
Coaching	2	8,70
Mentoring	2	8,70
Bases	1	4,35
E-learning	1	4,35
Clasificación	1	4,35
Clustering	1	4,35
TOTALES	23	100,00

Del análisis de la Tabla 4 y de la Tabla 5 presentadas anteriormente, surge que existe relación entre las etapas o fases de GC y las herramientas y técnicas que se mencionan en estas.

Se presenta a continuación en la Tabla 15 las etapas o fases de GC y las herramientas y técnicas que se mencionan en estas:

TABLA 15. AUTOR, ETAPAS, HERRAMIENTAS Y TÉCNICAS.

Autor	Etapas	Herramientas	Técnicas
Davenport	Generación	Redes, Fusión y Adquisición de conocimiento.	
	Codificación	Mapas y Patentes	Sistemas expertos
	Transferencia		Charlas informales, Contacto personal y Mentoring.
Probst	Identificación	Fusión o adquisición del conocimiento.	
	Adquisición	Lecciones aprendidas y grupos expertos.	
	Desarrollo	Comunidades de práctica, redes, mejores prácticas y análisis de redes sociales.	
	Compartir o Distribuir conocimiento.	Accesibilidad y diseño del área de trabajo.	
	Uso	Memoria organizacional.	
	Retención del conocimiento.		
Nonaka y	Socialización		Cámaras web, videoconferencias y realidad virtual.

Takeuchi	Externalización	Comunidades de práctica y grupos expertos.	
	Internalización		Bases de conocimiento y Elearning.
	Combinación de creación del conocimiento.		Clasificación y Clustering.

En relación a los factores encontrados, estos se clasificaron, inicialmente, en dos grupos, según fuera un factor de éxito o un factor de fracaso u obstáculo. Estos factores extraídos, fueron construidos en base a la similitud semántica de las denominaciones dadas a los factores reportados en los diferentes estudios analizados. Por otra parte, más de un artículo menciona los mismos factores, ya que fueron considerados en más de un estudio o reportados en más de un artículo.

El recuento de los factores encontrados dio un total de 45 resultados, discriminados en 23 factores de éxito, 21 factores de fracaso u obstáculos (13 factores de fracaso y 9 factores de obstáculos). Los factores incluidos en cada grupo tienen en común que afectan positiva o negativamente a la GC, más allá de los diferentes términos usados por los autores de los artículos revisados.

A continuación se muestra en la Tabla 16 los factores identificados en la literatura, sus definiciones según los autores que las mencionan y la cantidad de veces que son mencionados como factores de éxito o de fracaso u obstáculos:

TABLA 16. FACTORES, DEFINICIÓN, FACTORES DE ÉXITO, FACTORES DE FRACASO U OBSTÁCULOS Y TOTAL DE MENCIONES.

Factores	Definición	Cantidad de menciones como Factores de Éxito	Cantidad de menciones como Factores de Fracaso, obstáculos	Total de menciones
Recursos económicos	Refiere a la provisión de los recursos financieros necesarios para el desarrollo de las actividades de GC	13	17	30
Tiempo	Refiere a la dedicación de suficiente tiempo para las actividades de Gestión de conocimiento.	11	12	23
Capacitación	Refiere a la provisión de entrenamiento relativo a la mejora de la GC.	10	11	21
Recursos Humanos	Refiere a la provisión de las personas necesarias para el desarrollo de las actividades de GC.	14	13	27
Marcos Buenas practicas	Refiere a la existencia de un conjunto de formas de realizar determinada tarea para el logro de una eficiente GC.	12	4	16

Cultura organizacional	Refiere a la existencia de una forma de gestionar el conocimiento que sea entendida y aplicada por todos los miembros de la organización.	10	3	13
CKO	Refiere a la existencia de un director de Gestión de Conocimiento.	7	2	9
Compromiso de la alta gerencia	Refiere al compromiso y apoyo de los ejecutivos y de la alta gerencia a la GC.	10	10	20

Una vista global de ambos factores estudiados, factores de éxito y factores de fracaso u obstáculos mencionados por los autores, permite tener una visión global de su incidencia. En la Tabla 19 se observa que la mayor presencia la adquiere el factor “success” con el 51,11 % del total, seguido por el factor “failure” con el 28,89 % y en último lugar el factor “obstacles” con el 20 %.

TABLA 17. FACTORES, CANTIDAD Y PORCENTAJE DE ARTÍCULOS.

Tipo de Factores	Cantidad de Artículos	%
Success	23	51,11
Failure	13	28,89
Obstacles	9	20,00
TOTALES	45	100,00

FACTORES DE EXITO

Los factores críticos de Éxito de la GC, son definidos tal como los autores los definen en la literatura. Se presentan a continuación en la Tabla 18 donde se muestra la cantidad de menciones y los porcentajes de los mismos. El ordenamiento por cantidad de menciones da una indicación de la importancia relativa que los diferentes grupos de factores tienen en su incidencia en una iniciativa de mejora de GC.

TABLA 18. FACTORES, CANTIDAD Y PORCENTAJES DE ÉXITO.

Factores	Cantidad F. Éxito	%
Recursos Humanos	14	16,09
Recursos Económicos	13	14,94
Marcos Buenas Prácticas	12	13,79
Tiempo	11	12,64
Capacitación	10	11,49

Cultura Organizacional	10	11,49
Compromiso de la Alta Gerencia	10	11,49
CKO	7	8,05
TOTALES	87	100,00

FACTORES DE FRACASO Y OBSTÁCULOS

Los factores críticos de Fracaso y Obstáculos de la GC, son definidos tal como los autores los mencionan en la literatura. Se presentan a continuación en la Tabla 19 donde se muestra la cantidad y porcentajes de menciones de los mismos.

TABLA 19. Factores, cantidad y porcentaje de fracaso y obstáculos

Factores	Cantidad F. Fracaso y Obstáculos	%
Recursos Económicos	17	23,61
Recursos Humanos	13	18,06
Tiempo	12	16,67
Capacitación	11	15,28
Compromiso de la Alta Gerencia	10	13,89
Marcos Buenas Prácticas	4	5,56
Cultura Organizacional	3	4,17
CKO	2	2,78
TOTALES	72	100,00

IV. CONCLUSIONES Y TRABAJOS FUTUROS

Una GC eficiente implica conocer las etapas, herramientas, técnicas y factores que inciden en la misma. Es así que las organizaciones estarán en condiciones de potenciar los factores de éxito que inciden positivamente en la GC y minimizar aquellos que obstaculizan o inciden negativamente en esta, aplicando las herramientas y técnicas más apropiadas a la fase en la que se encuentran y visualizando las que deberían utilizar para el logro de la mejora continua, favoreciendo de esta manera a los objetivos del negocio de la organización.

En la literatura sobre GC en PyMEs existen una serie de estudios empíricos orientados a identificar estas etapas, herramientas, técnicas y factores que inciden en la misma.

El propósito de este artículo fue reportar los resultados de un mapeo sistemático de la literatura cuyo objetivo fue identificar y localizar la investigación existente sobre las etapas, herramientas, técnicas y factores de éxito, fracaso u obstáculos que afectan a la Gestión de Conocimiento.

El proceso seguido consistió en la definición de las preguntas de investigación, la búsqueda de la literatura relevante en una bases de datos bibliográfica, la definición de criterios de inclusión y exclusión para la selección de los estudios pertinentes, la clasificación de los estudios seleccionados en base a un conjunto de criterios previamente definidos y finalmente, la extracción y agregación de los datos.

Como resultado se obtuvo un conjunto de 32 estudios relativos al tema, de los cuales se extrajeron datos que permitieron determinar las fases, herramientas, técnicas y los tipos de factores a los que se enfocaron tales estudios, los métodos de investigación utilizados, los medios de divulgación utilizados para su publicación, los principales investigadores dedicados al tema, las principales publicaciones, la actividad de investigación en el tema y las revistas y conferencias en las que se han publicado o presentado la mayoría de los trabajos seleccionados.

A su vez se identificó a los autores que definen a las etapas, las herramientas y técnicas utilizadas en la GC, el significado de las mismas y la cantidad de menciones en la literatura para mostrar la relevancia de estas, descubriendo una interesante relación entre las etapas o fases de GC y las herramientas y técnicas que se utilizan en las mismas. También se identificó y definió los factores de éxito, fracaso u obstáculos presentes en la literatura que afectan positiva o negativamente la GC y su cantidad de menciones para mostrar la relevancia de los mismos.

Es importante mencionar que, si bien los estudios seleccionados se obtuvieron siguiendo estrictamente el protocolo descrito en la sección 2, la inclusión de otras bases de datos bibliográficas y de otros sinónimos de las palabras claves de búsqueda permitan encontrar artículos adicionales sobre el tema.

Como trabajo futuro se realizará un estudio de investigación sobre la situación de la GC en empresas PyMEs de la República Oriental del Uruguay, donde se evaluará de qué manera intervienen las etapas, herramientas, técnicas y factores críticos de éxito, fracaso u obstáculos identificados en la literatura, pudiendo obtener nuevas evidencias sobre estos, así como la identificación de otros elementos y características propias de estas empresas aún no identificadas en la literatura existente.

REFERENCIAS

- [1] L. Paradela, "Una metodología para la gestión del conocimiento," Tesis Doctoral, Facultad de Informática, Universidad Politécnica de Madrid, Madrid, España, 2001.
- [2] A. Del Moral, J. Pazos, E. Rodríguez, R.-P.A, and S. Suarez, Gestión del conocimiento. Madrid, España: Paraninfo, 2007.
- [3] U. DINAPYME, Equipos Mori, Consultores Asociados, "Encuesta Nacional de mPyMEs industriales y de servicios," 2013.
- [4] H. Mintzberg, Diseño de organizaciones eficientes. Buenos Aires: El Ateneo, 1989.
- [5] Petticrew, M. and H. Roberts, Systematic reviews in the social sciences. A practical guide, 2006, Malden, MA: Blackwell.
- [6] Kitchenham, B.A., D. Budgen, and O.P. Brereton, Using mapping studies as the basis for further research. A participant- observer case study. *Information and Software Technology*, 2011. 53: p. 638–651.
- [7] Petersen, K., et al., Systematic Mapping Studies in Software Engineering, in 12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 2008: Bari, Italy.
- [8] Arksey, H. and L. O'Malley, Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology*, 2005. 8(1): p. 19-32.
- [9] Auster, E., K. Wylie, and M. Valente, Strategic Organizational Change. Building Change Capabilities in your Organization, 2005, Hampshire: Palgrave Macmillan.
- [10] Gerhardt, M., D. Frey, and P. Fischer, The human factor in change processes: Success factors from a socio-psychological point of view, in Change 2.0. Beyond Organisational Transformation, J. Klewes and R. Langen, Editors. 2008, Springer: Berlin.
- [11] A. Gomez, N. Juristo, C. Montes, and J. Pazos, Ingeniería del conocimiento. Madrid, España: Centro de Estudios Ramón Areces, S.A., 1997.
- [12] T. Davenport, G. Probst and L. Prusac. Working knowledge: how organizations manage what they know. Boston, MA: Harvard Business School Press, 1998.
- [13] I. Nonaka and H. Takeuchi, Modelo SECI. Nueva York: USA: Oxford University Press, 1995.
- [14] G. Probst, S. Raub, and K. Romhardt, Administre el conocimiento. México: Pearson, 2001.
- [15] I. Nonaka and H. Takeuchi, La organización creadora de conocimiento. México D.F, México: Oxford University Press, 1999.
- [16] R. Bergmann, Experience management. Berlín: Springer, 2002.
- [17] I. Nonaka, H. Takeuchi, The Knowledge creating company: How Japanese companies create the dynamis of innovation. 1995.
- [18] T. Davenport, D. DeLong, and M. Beers, Successful Knowledge management projects. Boston, MA: Harvard Business School Press, 1998.
- [19] Chen Hongmei, Miao Yujun, Knowledge Management for SMEs Based on the Balanced Scorecard, Sch. Of Econ. & Manage., Qiqihar Univ., Qiqihar, China, 2010.
- [20] Qi Guiqing, Yang Xihuai, Xiao Zhuo, Building the Competitive Advantage of SMEs in High-tech Industry on Knowledge Management View, Sch. of Bus. Adm., Northeastern Univ., 2006.
- [21] R. Cross and L. Baird, "Technology is not enough: Improving performance by building organizational memory.", 2000.
- [22] Norkjaer, M.A., Scheel, H. ; Sorensen, M.A.S., Why early implementation of a Knowledge Management System can support the growth of R&D-driven SMEs, Inst. of Bus. & Technol., Univ. of Aarhus, Herning, Denmark, 2010.
- [23] Fang Luo, Determinants of knowledge search strategy of Chinese SMEs, Sch. of Manage., Zhejiang Univ., Hangzhou, China, Industrial Engineering and Engineering Management (IEEM), 2010 IEEE International Conference on, 2010.

- [24] Nagi, K., Use of moodle reports for knowledge management, planning and eTraining in SMEs, Coll. of Internet Distance Educ., Assumption Univ., Bangkok, 2008.
- [25] M. Jennex, Olfman, L. , "Organizational memory/knowledge effects on productivity, alongitudinalstudy.", 2002.
- [26] E. Wenger, McDermott,R., Snyder,W. , "Cultivating communities of practice.", 2002.
- [27] Bandini, S., Manzoni, S. ; Sartori, F., Case-Based Reasoning to Support Work and Learning in Small and Medium Enterprises, DISCo Dept. of Comput. Sci., Syst. & Commun., Univ. of Milano-Bicocca, Milan, Italy, 2009.
- [28] Yuanhong Liao, Lili Qi, Knowledge Management System in Project-Based Organizations, Coll. Of Econ.&Manage., China Agric. Univ.(CAU), Beijing, China, 2009.
- [29] Portera-Zanotti, N. ; Rinsche, T., Innovative knowledge management practices for SMEs, Information Society (i-Society), 2010 International Conferenceon, 2010.
- [30] Noudoostbeni, A., Yasin, N.M. ; Jenatabadi, H.S., A Mixed Method for Training ERP Systems Based on Knowledge Sharing in Malaysian Small and Medium Enterprise (SMEs), Dep. Inf. Sci., Univ. Malaya, Kuala Lumpur, 2009.
- [31] Murni, H.F. , Siregar, L. ; Budiarto, R., Evaluating the Best of Knowledge Management Technology for Small Medium Enterprise Based on Fuzzy Analytic Hierarchy Process, Sch. of Comput. Sci., Univ. Sains Malaysia, Minden, 2009.
- [32] Abbaszadeh, M.A., Ebrahimi, M. ; Fotouhi, H., Developing a causal model of critical success factors for knowledge management implementation, Dept. of Ind., Persian Gulf Univ., Bushehr, Iran, 2010.
- [33] Mahmod, R., Rosnan, H. ; Hazman-Fitri, M.H., Knowledge management and innovation readiness among SMEs in Malaysia, Fac. of Bus. Manage., Univ. Teknol. MARA, Puncak Alam, Malaysia, 2013.
- [34] Trivedi, P., Dubey, A. Implementation of KM in Indian SMEs: modeling the variables, Amity Sch. of Eng. &Technol., Amity Univ., Lucknow, India, 2012.
- [35] MoonKoo Kim, JongHyun Park ; JongHyun Paik, An empirical analysis to strengthen the knowledge management capability in Korea SMEs, Future Strategy Res. Team, ETRI, Daejeon, South Korea, 2011.
- [36] Wei Long, Olufemi, E.A., Knowledge Management and Innovation for Firms Competitiveness: A Strategic Approach for African SMEs, Sch. of Econ., Wuhan Univ. of Technol., Wuhan, China, 2011.
- [37] Mesaric, J., Knowledge management - necessity and challenge in small and medium enterprises, Fac. of Econ., Univ. JJ. Strossmeyer, Osijek,2004.
- [38] JingTian, Nakamori, Yoshiteru, Consideration on a service system for knowledge management in scientific laboratories, Sch. of Knowledge Sci., Japan Adv. Inst. of Sci. &Technol., Japan "2005.
- [39] Hamburg, I., eLearning 2.0 and Social, Practice-Oriented Communities to Improve Knowledge in Companies, Inst. for Work & Technol., FH Gelsenkirchen, Gelsenkirchen, Germany, 2010.
- [40] Beierle, Cristoph, Meghini, Carlo, Foundations of Information and Knowledge Systems, 8th International Symposium, Folks 2014, Proceedings Series of lecture notes in Computer Science., Bordeaux, France, 2014.

ANEXO III - Modelo de Madurez de Alineamiento Estratégico de TI en empresas de tipo PyMEs y resultados de la aplicación de este modelo en estas organizaciones

Caso de Estudio : Uruguay

Helena Garbarino Alberti
garbarino@ort.edu.uy
Facultad de Ingeniería
Universidad ORT Uruguay
Montevideo, Uruguay

Sebastián Ayala
ayala_s@ort.edu.uy
Facultad de Ingeniería
Universidad ORT Uruguay
Montevideo, Uruguay

José Carrillo Verdún
jcarrillo@fi.upm.es
Facultad de Informática
Universidad Politécnica de Madrid
Madrid, España

Resumen

El artículo presenta un modelo de madurez para medir el alineamiento estratégico de TI en organizaciones de tipo PyME de Uruguay. Este modelo se desarrolló a través de un estudio empírico acerca de la gobernanza corporativa de las tecnologías de la información realizado en la República Oriental del Uruguay a pequeñas y medianas empresas para medir el alineamiento estratégico de TI en estas organizaciones. El análisis de las organizaciones encuestadas fundamentó el desarrollo de un nuevo modelo de madurez exclusivo para PyMEs de Uruguay. Se presenta el modelo de madurez desarrollado, y los resultados de su aplicación en organizaciones de tipo PyMEs, en este caso de Uruguay.

Palabras Claves

Gobierno Corporativo de TI, PyMEs, Alineamiento estratégico, Modelo de madurez.

Abstract

This article introduces a maturity model meant to measure the strategic alignment of IT in SME type organizations in Uruguay. It has been developed through an empirical study conducted in La República Oriental del Uruguay on Corporate Governance of Information Technology, to measure the IT strategic alignment present in these organizations. Analysis made on the surveyed organizations, provided the foundation for the development of a new maturity model that fits SMEs in Uruguay. This developed maturity model and its application in SME organizations -of Uruguay in this case- is hereby presented.

Index Terms

IT Corporate Governance; SMEs; Strategic alignment; Maturity model.

I. INTRODUCCIÓN

En un mundo cambiante y competitivo, en el que las empresas necesitan de la tecnología para poder competir y obtener beneficios a corto y largo plazo, las pequeñas y medianas empresas conforman un ámbito particular de estudio ya que no comparten algunas de las características de las grandes corporaciones. Es en éste ámbito en el que se realiza un estudio empírico acerca de la madurez de la gobernanza corporativa de las tecnologías de la información (de aquí en más GCTI) en el área de alineamiento estratégico de TI en Uruguay. A partir de este estudio se construye un modelo que permite medir adecuadamente la madurez de las organizaciones de tipo PyME (pequeñas y medianas empresas) de Uruguay en el área de alineamiento estratégico de TI.

Según Weill y Ross [1] alineamiento estratégico es alinear las estrategias de TI de una organización con su estrategia general para que ésta alcance su meta y objetivo, y constituye uno de los cinco componentes fundamentales del Gobierno de TI.

Actualmente existen varios marcos de buenas prácticas y estándares internacionales para el Gobierno de TI: COBIT (IT Governance Institute, 2012), Val IT (IT Governance Institute, 2008), ITIL (U.K. Office of Government Commerce, 2007), ISO 38500 (IT Governance Institute, 2008), Calder Moir (Calder y Moir, 2009) y MOF (Microsoft Corporation, 2008).

A partir del análisis de la información recabada a través de un trabajo de campo diseñado específicamente para este estudio se elabora un modelo de madurez, derivado de los presentados por los marcos anteriormente citados, adaptándolos a la realidad particular de las PyMEs de Uruguay. La integración de los distintos modelos de madurez para alineamiento estratégico de TI no es tarea sencilla y surge del estudio realizado que su aplicación a las PyMEs de Uruguay presenta desafíos adicionales a los de su implantación en empresas de mayor porte. En este caso, es imprescindible evitar la sobrecarga de procedimientos y prácticas, apuntando a mantener un marco de trabajo y un modelo de madurez simple y eficaz.

El artículo está organizado en diez secciones, donde la primera es la introducción, en la segunda se define el contexto del gobierno corporativo y su historia, en la tercera sección se da contexto a las tecnologías de información, en la sección cuarta se define el contexto de las empresas PyMEs en la República Oriental del Uruguay, el contexto del Gobierno de TI y sus marcos así como las características e importancia de las pequeñas y medianas empresas en la economía uruguaya. En la sección quinta se presentan los objetivos del trabajo de campo presentando su metodología en la sección seis. Las secciones siete, ocho, nueve y diez presentan los resultados obtenidos, el Modelo de Madurez del Alineamiento de TI en las Pymes de Uruguay, el Análisis de los niveles de madurez de las Pymes, y las conclusiones y trabajos futuros.

II. CONTEXTO DEL GOBIERNO CORPORATIVO

En los últimos años, escándalos y fraudes tales como los de Enron, Worldcom y Tyco (2002) entre otros han impulsado el desarrollo de códigos de buen gobierno corporativo que garanticen una gestión transparente, la estabilidad de los mercados financieros, la inversión y el crecimiento económico [2]. Estos códigos, leyes y modelos han evolucionado a lo largo del tiempo, distinguiéndose entre otros en Europa: el Informe Cadbury (Reino Unido, 1992); el Código Olivencia de Buen Gobierno (España, 1998); el Informe Winter: Report of the High Level Group of Company Experts on a Modern Regulatory Framework for Company Law in Europe (2002); el Informe Aldama (España, 2003); el Company Law and Corporate Governance y la Comisión Europea: Mercado Interior. A nivel internacional se destacan: el Principles of Corporate Governance: analysis and Recommendations (1992); los Principios de la OCDE (Organización para la Cooperación y el Desarrollo Económico) para el Gobierno de las sociedades (1999); el European Corporate Governance Institute; la Comisión Nacional del Mercado de Valores (España) y el código Sarbanes-Oxley (EEUU, 2002) (datos obtenidos del “Corporate Governance, Dossier de Recusos” [3]). En el Uruguay la entidad reguladora de dichos principios es el Banco Central del Uruguay (BCU) a través del documento: “Instituciones de intermediación financiera - Normativa sobre gobierno corporativo y sistema de gestión integral de riesgos” cuya última versión es del año 2008 [4].

III. CONTEXTO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

La información y las tecnologías de la información (de aquí en adelante TI) forman parte del conjunto de activos clave en las organizaciones ya que habilitan la consecución de valor incidiendo tanto en aspectos internos como externos, en sus procesos, productos y comunicaciones, añadiendo valor a sus actividades y habilitando su eficacia y su eficiencia [5]. Esto se ve apoyado en los resultados empíricos obtenidos por los autores Weill y Ross los que han dado lugar al modelo propuesto por dichos autores y publicado en el libro “IT Governance. How top performers manage IT decision rights for superior results” [1].

Las organizaciones deben tomar cinco tipos de decisiones en lo que respecta a Tecnologías de la Información [1]:

- 1) Decisiones de principios de TI: son aquellas que establecen el rol de las TI en la compañía.
- 2) Decisiones de arquitectura de las TI: son aquellas que determinan las elecciones técnicas en TI.
- 3) Decisiones de infraestructura de TI: son aquellas que determinan la organización física de las piezas de hardware de la organización.
- 4) Decisiones de aplicaciones de negocio: son aquellas que determinan las especificaciones y requerimientos para las aplicaciones de negocio a desarrollar en la organización, que darán soporte a los procesos de negocio.
- 5) Decisiones de priorización y de inversiones en TI: son aquellas que determinan en que proyectos o recursos de TI invertir y que infraestructura adquirir.

Es muy importante que los directores de la empresa reconozcan la responsabilidad que tienen en la toma de decisiones y el uso y manejo efectivo de TI y no asuman que la responsabilidad es del departamento de TI, de aquí que, el ITGI, define al gobierno de TI como: “El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que TI en la empresa sostiene y extiende las estrategias y objetivos organizacionales”[5]. Las actividades de Gobierno de TI pueden ser agrupadas en las siguientes cinco áreas de enfoque, las cuales se detallan a continuación [5]:

- 1) Alineamiento Estratégico. Se enfoca en asegurar el enlace de los planes del negocio y de TI; en definir, mantener y validar la proposición de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa. Asegura que la inversión en TI de una empresa está acorde con los objetivos estratégicos de la misma.
- 2) Entrega de Valor. Se refiere a ejecutar la proporción de valor a través de todo el ciclo de entrega, asegurando que TI entrega los beneficios acordados alineados con la estrategia, concentrándose en la optimización de costos, y demostrando el valor específico de TI.
- 3) Administración de Riesgos. Se realiza a través de mitigar, transferir, aceptar y evitar. Para ello se requiere conciencia de riesgo por parte de los directores superiores de la empresa, entendimiento del apetito del riesgo de la empresa, transparencia sobre los riesgos significativos de la empresa e implementar las responsabilidades de la administración de riesgos dentro de la organización.
- 4) Administración de Recursos. Se refiere a la inversión óptima y la adecuada administración de los recursos críticos de TI (aplicaciones, información, infraestructura, personas).

5) Medición del Desempeño. Da seguimiento y supervisa la estrategia de implementación, la finalización de proyectos, el desempeño de procesos y la entrega de servicio, ya que lo que no se puede medir, no se puede administrar.

De acuerdo con Peter Weill y Jeanne Ross [6] en una economía digital, las TI son la base de los negocios, por lo que, los CEOs (Chief Executive Officer, en español, Director ejecutivo) o en el contexto de una empresa mediana, aquel que toma las decisiones debería preguntarse:

- 1) ¿Estamos utilizando la tecnología para transformar nuestro negocio, o solo estamos agregando campanas y silbatos a los procesos existentes?
- 2) ¿Estamos ignorando las diferencias importantes del negocio como estandarizar procesos en toda la empresa?
- 3) ¿Quién se asegura que la estrategia digital de la compañía se está aplicando?
- 4) ¿La información electrónica está capacitando a su personal o solo controlándolo?

Todos estos elementos hacen al contexto de las TI, su gobernanza y la obtención de valor a través de la misma.

IV. CONTEXTO DE EMPRESAS PYMES EN LA REPÚBLICA ORIENTAL DEL URUGUAY

La realidad del mercado industrial en el Uruguay hace que las empresas categorizadas como PyMEs[7] tengan una incidencia fundamental; según la DINAPYME (Dirección Nacional de Artesanías, Pequeñas y Medianas Empresas. Ministerio de Industria, Energía y Minería)[8] el 99% de las unidades económicas productivas del sector privado del Uruguay son PyMEs y el 70% de las personas trabaja en empresas tipificadas como tales [9].

En el Uruguay, se considera como pequeña empresa a las de hasta 19 trabajadores y mediana empresa a las que poseen entre 20 y 99. Esta clasificación varía según el país que se considere, siendo en general mayores los límites de cada intervalo a mayor tamaño del país y volumen económico.

Esta particularidad hace que sea altamente relevante analizar elementos de gobierno de TI aplicados a este tipo de empresas. Éste tipo de empresa aporta el 33% de PBI y el 25% de la inversión [10]. También las PyMEs son muy importantes en las distintas economías del mundo. Estadísticas de la SBA (U.S. Small Business Administration) de Estados Unidos muestran que en el 2007 las pequeñas empresas generaron alrededor del 50% de todas las ventas estadounidenses, y también contribuyeron al 50 % del PBI privado. Además, emplearon a más del 50% de la fuerza laboral de ese país [11].

V. ESTADO DEL ARTE DEL GOBIERNO CORPORATIVO DE TI

En conjunción con lo anterior, se han creado marcos de Gobierno Corporativo de las Tecnologías de la Información (de aquí en más GCTI) que garanticen el control de la información, la obtención de valor como consecuencia de la alineación estratégica entre los objetivos del negocio y los de TI, la gestión de los recursos y de los riesgos asociados a TI, así como la calidad de los servicios entregados. Es en este sentido que surgen los siguientes marcos: los propuestos por el ITGI (Information Technology Governance Institute): el marco COBIT (Control Objectives for Information and related Technology) 4.1 [5], el marco Val IT (Marco de trabajo para el gobierno del valor. Creado por el ITGI)[12] y el Risk IT (– Marco de trabajo para el gobierno del riesgo. Creado por el ITGI) [13-14] (Al momento de escribir este documento no ha sido publicada la nueva versión del marco COBIT (la versión 5.0) la cual promete unificar los tres marcos mencionados anteriormente en un modelo de Gobierno Corporativo de TI), el marco propuesto por el CISR [1] (CISR - Center for Information Systems Research, MIT), el propuesto por Van Grenbergen[15], el ISO 38.500 [16], el marco Calder-Moire[17] y el marco Forrester[18].

Ejemplos comerciales como el publicado por InfoWeek[19], hace referencia directa a la importancia de las PyMEs en América Central y del Sur y de las inversiones en TI que las mismas realizan; en el ámbito europeo, el estudio realizado por el Aula TIC-PyMEs de la Universidad de Santiago de Compostela [20] donde se categoriza la importancia del uso de las tecnologías por tamaño/sector; otros estudios, como el realizado por Arroyo y Carrillo [21] respecto del uso de TICs y de la existencia/madurez de gobierno de TI en PyMEs españolas enfatizan la importancia de las TI y las debilidades existentes en la gestión de las mismas. Las características de las PyMEs les permiten mayor flexibilidad y mayor velocidad de respuesta frente a cambios en el sector donde se desarrollan, y es en éste sentido que la adopción de nuevas tecnologías puede contribuir a la obtención de mayores beneficios optimizando los procesos a lo largo de toda la cadena.

VI. OBJETIVOS DEL ESTUDIO DE CAMPO

El presente estudio no está enmarcado en ningún proyecto de carácter general ni gubernamental por lo que los objetivos del mismo son específicos al área y a la propia investigación. Los objetivos son: realizar un diagnóstico de la situación de la GCTI y a partir del mismo identificar los principales problemas y cuantificar adecuadamente los recursos que disponen estas organizaciones para abordar la implantación de buenas prácticas de Gobierno de TI y de alineamiento estratégico. El análisis de los datos recogidos en este trabajo permitió la identificación de características comunes, la clasificación de las organizaciones de acuerdo a las diferentes variables observadas, y la identificación de aquellas buenas prácticas COBIT [14] y Val IT [12] aplicable a la realidad de las PyMEs de Uruguay fundamentando el desarrollo del modelo de madurez específico para PyMEs en el Uruguay.

VII. METODOLOGÍA

Se analizaron 30 organizaciones entrevistando a Directores Generales, Directores Financieros, Directores de Departamento y Directores de TI de pequeñas y medianas empresas (hasta 100 trabajadores). La técnica utilizada fue la entrevista personal, con una duración aproximada de 45 minutos.

Se definió una muestra no probabilística de criterio intencional [22], en la que el tipo de selección que primó es el criterio personal del investigador acerca de la representatividad y heterogeneidad de la población que se está estudiando. Por ello la selección incluyó una distribución heterogénea de rubros, tipos de empresas (industriales y de servicios), y zonas del país (departamentos de Montevideo, Maldonado, San José y Colonia) [23].

1. Margen de Error: No se puede calcular el error de la muestra por tratarse de una muestra no probabilística.
2. Sujeto Encuestado: Fueron encuestados Directores Generales, Directores Financieros, Directores de Departamento y Directores de TI de las empresas.
3. Unidad de Análisis: El análisis se centró en las PyMEs (pequeñas y medianas empresas).
4. Universo: El universo de análisis son las PyMEs (pequeñas y medianas empresas).
5. Procesamiento de la información Las encuestas fueron codificadas e ingresadas a una base de datos que se depura controlando inconsistencias. La información se procesó mediante un programa informático estadístico SPSS.
6. Alcance del Estudio El informe presentado corresponde a los resultados de la aplicación de la encuesta realizada durante los meses de julio – agosto de 2010.
7. Resultados de Campo: Del total de contactos efectuados, 100% constituyeron entrevistas efectivas, no existiendo ningún rechazo.

VIII. RESULTADOS

A continuación se presentan los resultados obtenidos relativos a cada una de las áreas del gobierno de TI:

A. Gobierno de TI

En nueve de cada diez organizaciones no hay ningún conocimiento de Gobernanza de TI.

Según el estudio realizado, el alineamiento estratégico de TI con los objetivos del negocio en las empresas encuestadas es el siguiente: 2 de cada 3 empresas (65%) está en los niveles 1 y 2 de madurez (la escala de niveles es de 1 a 5).

B. Toma de decisiones

La figura 1 muestra que en 1 de cada 2 organizaciones (50%) las decisiones de TI son tomadas únicamente por el gerente o director general y solo en un 2 % por el conjunto de directores de la empresa.

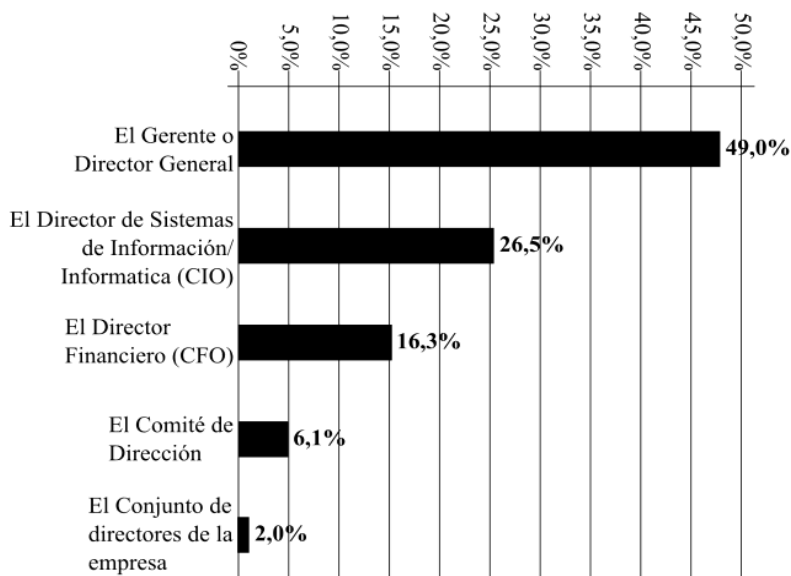


Figura 1. Toma de decisiones sobre TI

C. Estructura de TI

Sólo en 1 de cada 3 (33%) la planificación de la estrategia de TI es determinada con participación del director de sistemas y del director financiero además del director general como se muestra en la figura 2.

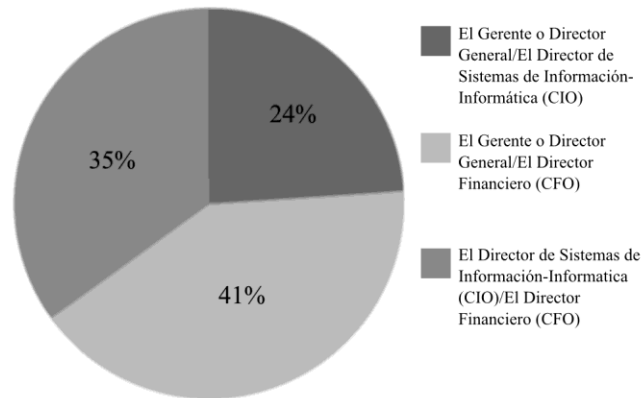


Figura 2. Responsable de la planificación de la estrategia de TI

D. Valor de TI

En la mayoría de las organizaciones (64%) se percibe a TI solo como un soporte operativo al negocio, no existiendo responsabilidades definidas en TI y no valorizando la importancia que tiene TI para apoyar y lograr el cumplimiento de los objetivos del negocio así como la mejora continua del mismo.

En general no se corresponde la importancia que los empresarios dicen asignarle a TI como elemento que permite la consecución de una estrategia (65% la considera imprescindible) en relación a los gastos del presupuesto asignados a TI (47% le asigna entre un 5 y un 10%) tal como podemos apreciar en la tabla 1 y en la figura 4.

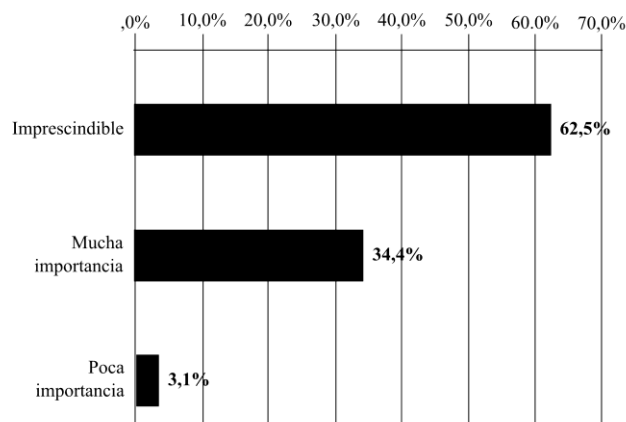


Figura 3. Importancia de TI en la organización

TABLA 1. PRESUPUESTO ASIGNADO A TI

% de Presupuesto	% de casos
5	23,1
10	23,1
3	7,7
8	7,7
15	7,7
25	7,7
30	7,7
40	7,7
50	7,7

El 40% de las organizaciones no mide el valor que le aporta TI al negocio.

E. Riesgos y seguridad de TI

Solamente 1 de cada 3 organizaciones (30%) realizan una gestión de riesgos en el área de seguridad de la información.

El 70% de las empresas no cuenta con un plan de recuperación de desastres. El restante 30% se caracteriza por si poseer un plan de contingencia tal como podemos apreciar en la figura 5.

F. Servicios de TI

- La mayoría de las organizaciones (83%) no ha definido los servicios que TI debe brindar a la organización.
- La mayoría de las organizaciones (86%) no monitorea la calidad ni el cumplimiento de los servicios de TI.
- La mayoría de las organizaciones (93%) no han implementado acuerdos de tipo SLA (Service Level Agreement) para los servicios de TI.
- Ninguna de las empresas ha implementado acuerdos de tipo SLA para los servicios contratados a terceros.

IX. MODELO DE MADUREZ DEL ALINEAMIENTO DE TI EN LAS PYMES DE URUGUAY

Se desarrolló un modelo de madurez para medir el alineamiento de los objetivos de TI con los objetivos estratégicos de las PYMES que podemos apreciar en la tabla 2. Este modelo se compone, a semejanza de los modelos de madurez más conocidos (COBIT (IT Governance Institute, 2007), ValIT (IT Governance Institute, 2007), CMM (SEI.1993), etc.) de una escala ascendente con cinco niveles de madurez. Cada nivel representa un modelo de empresa PYME con determinados atributos de madurez en diferentes áreas de TI, identificados a partir de nuestro trabajo de investigación de campo. Cada nivel del modelo contiene implícitamente los atributos del nivel inmediato anterior.

En el modelo, los niveles se representan en filas de una matriz de atributos, comenzando por el nivel uno y llegando hasta el nivel cinco. Se identificaron las siguientes seis áreas, que se representan en columnas de la matriz, como objetivos estratégicos de la organización. Estructura de TI. La estructura física, lógica, y la dimensión de los recursos de TI de una organización tienen un impacto directo sobre la aplicabilidad o no de determinadas buenas prácticas que requiere la alineación de TI con el negocio.

Valor de TI. El valor entregado por los productos y servicios de TI a la organización incide de manera directa en la capacidad de consecución de los objetivos estratégicos de la misma. TI puede estar correctamente alineada con los objetivos del negocio pero si falla en su entrega de valor dificulta la consecución de los mismos.

Servicios de TI. La correcta gestión de los servicios provistos por TI, es decir de los niveles de calidad de los mismos, la distribución de los costos y responsabilidades, la entrega de valor para los usuarios y el negocio, son fundamentales para hacer efectiva una buena alineación de TI con el negocio.

Riesgos y Seguridad de TI. La gestión de los riesgos y la seguridad de los servicios y activos de TI son imprescindibles para permitir la continuidad del negocio y en algún caso puede incidir directamente en la consecución de los objetivos del negocio.

Toma de Decisiones. El involucramiento los directores o gerentes de las distintas áreas o departamentos de una organización en la definición y planificación de los objetivos de TI incide directamente en el alineamiento de TI con los objetivos del negocio. A mayor participación y grado de involucramiento, mejor es el alineamiento de TI con el negocio.

Gobierno de TI. La aplicación de buenas prácticas y marcos de Gobierno de TI redundan en una mejor administración, control, y gestión de los recursos de TI, e incluyen prácticas y procesos específicos para mejorar el alineamiento estratégico de TI con el negocio.

Luego presentamos tablas donde identificamos las relaciones entre distintos atributos del modelo de madurez y los procesos y prácticas de los marcos COBIT (IT Governance Institute, 2012) y ValIT (IT Governance Institute, 2008). A través de este análisis podemos apreciar las prácticas que necesitan ser emprendidas o mejoradas en cada nivel del modelo de atributos de madurez de alineamiento estratégico de TI.

NIVEL 5 OPTIMIZADO	<ul style="list-style-type: none"> • Los procesos se han optimizado para mejorar el desempeño y la eficacia. • Existe un proceso de mejora continua, y una automatización de tareas que permite optimizar el flujo de trabajo y la disponibilidad de la información. • Se han identificado, gestionado, y minimizado los riesgos inherentes a TI y relativos a la continuidad del negocio. • La alineación entre TI y los objetivos estratégicos de la organización es la máxima posible. • Todos los sectores de la organización intervienen en la planificación de los objetivos e inversiones de TI.
-----------------------	--

A. Matriz de atributos de madurez del modelo

A modo de ejemplo se presentan las tablas de atributos de madurez para las áreas de Estructura de TI y Valor de TI. Análogamente se desarrollaron tablas de atributos de madurez para las áreas de Servicios de TI, Riesgos y Seguridad de TI, Toma de Decisiones de TI, y Gobierno de TI.

TABLA 3. ATRIBUTOS DE MADUREZ, ÁREA ESTRUCTURA DE TI.

Nivel	Estructura de TI
1	a. La mínima para dar algún grado de soporte operativo al negocio.
2	a. La necesaria para dar soporte operativo al negocio.
3	a. La estructura de TI da soporte a todas las áreas y/o departamentos de la organización. b. Existen roles y responsabilidades claramente definidos. c. Existen procesos y tareas de TI claramente definidos.
4	a. Existe un departamento de TI interno con una estructura claramente definida y RRHH suficientes para dar soporte al negocio. b. Existen estructuras organizativas adecuadas para supervisar y dirigir todos los recursos de TI de la organización. c. Existen procesos regulares de capacitación de los RRHH de TI y de entrenamiento de usuarios. d. La función de TI, sus relaciones con otros departamentos, y su ubicación organizacional están claramente definidos.
5	a. Existen procesos definidos para analizar tecnologías nuevas o existentes y su aplicación al negocio. b. Existe una planificación de infraestructura tecnológica que toma en cuenta los objetivos estratégicos de la organización y la continuidad del negocio. c. Los procesos de TI se auditan regularmente para asegurar su efectividad y desempeño.

TABLA 4. ATRIBUTOS DE MADUREZ, ÁREA VALOR DE TI.

Nivel	Valor de TI
1	<p>a. No se mide ni se cuantifica.</p> <p>b. Las inversiones en TI son las mínimas necesarias y muy conservadoras.</p> <p>c. No existe ninguna estrategia de TI.</p>
2	<p>a. No se mide ni se cuantifica.</p> <p>b. Las inversiones en TI son las necesarias y orientadas a la funcionalidad operativa del negocio.</p> <p>c. No hay una planificación de las inversiones en TI más que para cubrir las necesidades inmediatas del negocio.</p>
3	<p>a. No se realizan mediciones formales, aunque se cuantifica de manera estimativa.</p> <p>b. Las inversiones en TI son las necesarias para cubrir la funcionalidad operativa del negocio, y, en algún caso aislado pueden aplicarse a tecnologías innovadoras.</p> <p>c. Existe una planificación de inversión en TI enfocada en el corto y mediano plazo.</p> <p>d. Eventualmente, dependiendo del proyecto TI informa a la dirección sobre nuevas oportunidades de negocio.</p> <p>e. Se realiza un análisis de viabilidad (business case) identificando costos, beneficios, y departamentos afectados para todos los proyectos y servicios de TI.</p>
4	<p>a. Las inversiones en TI se gestionan como una cartera de inversiones.</p> <p>b. Las inversiones en TI están enfocadas a obtener el máximo valor posible para el negocio con una visión a mediano y largo plazo.</p> <p>c. TI informa regularmente a la dirección sobre nuevas oportunidades de negocio.</p> <p>d. Se incluyen en las inversiones de TI la relación de actividades que son requeridas para la obtención de valor para el negocio.</p> <p>e. Existe un presupuesto anual específico para TI.</p>
5	<p>a. Se gestionan las inversiones de TI en todo su ciclo de vida económico.</p> <p>b. Las inversiones en TI han aportado valor sustancial a la organización y ese valor es medido y cuantificado por la organización.</p> <p>c. Existe un procedimiento estándar para la selección, análisis, y priorización de las inversiones de TI.</p> <p>d. Se utilizan herramientas automatizadas y técnicas estándar de análisis de viabilidad de los proyectos e inversiones en TI.</p>

Vinculación entre procesos y prácticas de COBIT, ValIT y atributos de madurez de la matriz.

A continuación se presentan tablas donde se identifican las relaciones entre distintos atributos del modelo de madurez y los procesos y prácticas de los marcos COBIT (IT Governance Institute, 2012) y ValIT (IT Governance Institute, 2008).

Cada celda de la matriz contiene varios atributos o prácticas de TI que reflejan la aplicación o no de determinado proceso en un determinado nivel y su justificación.

El proceso definido por COBIT (IT Governance Institute, 2012) o ValIT (IT Governance Institute, 2008) puede no estar (y en general no lo está) contenido totalmente en la lista de atributos de una celda, pero cada uno de los atributos o prácticas tiene una vinculación directa con una o más de las actividades definidas por el proceso COBIT (IT Governance Institute, 2012) o ValIT (IT Governance Institute, 2008) correspondiente.

A través de este análisis se pueden apreciar las prácticas que necesitan ser emprendidas o mejoradas en cada nivel del modelo de atributos de madurez de alineamiento estratégico de TI. A modo de ejemplo se incluyen procesos para COBIT (IT Governance Institute, 2012) y para VALIT (IT Governance Institute, 2008) en las tablas aunque se analizan todos los procesos de ambos marcos (tabla 5).

TABLA 5. MAPEO DE PROCESOS DE COBIT QUE APLICAN AL MODELO

Procesos o Actividades definidas por COBIT	Ubicación en la matriz de atributos	Justificación
P01.2 – Alineación de TI con el negocio	- Valor de TI Nivel 4 ítem c. - Valor de TI Nivel 5 ítems b y c.	Planear y Organizar, Proceso P01 – Definir un plan estratégico.
P01.3 – Evaluación del desempeño y la capacidad actual	- Servicios de TI Nivel 5 ítem a. - Gobierno de TI Nivel 4 ítems b y c. - Gobierno de TI nivel 5 ítem b.	
P01.4 – Plan estratégico de TI	- Valor de TI Nivel 4 ítems a, d y e. - Gobierno de TI Nivel 4 ítem b.	
P03.1 – Planeación de la Dirección Tecnológica	- Riesgos y Seguridad de TI Nivel 3 ítem d. - Estructura de TI Nivel 4 ítem c. - Estructura de TI Nivel 5 ítem a. - Valor de TI Nivel 4 ítem c.	Planear y Organizar, Proceso P03 – Determinar la dirección tecnológica.
P03.2 – Plan de Infraestructura Tecnológica	- Valor de TI Nivel 5 ítem c. - Estructura de TI Nivel 5 ítem b.	
P04.1 – Marco de Trabajo de Procesos de TI	- Servicios de TI Nivel 4 ítem c. - Estructura de TI Nivel 5 ítem c.	Planear y Organizar, Proceso P04 – Definir los procesos, Organización y Relaciones de TI.

TABLA 6. MAPEO DE PROCESOS DE COBIT QUE NO APLICAN AL MODELO

Proceso y Práctica	Justificación
P03.3 – Monitoreo de Tendencias y Regulaciones Futuras	Los RRHH, económicos, y la estructura de TI requeridos por esta actividad están muy por encima de los disponibles para la - mayoría de las PyMEs en Uruguay.
P03.4 – Estándares Tecnológicos P03.5 – Consejo de Arquitectura de TI	- El ROI de una actividad de este tipo no justifica la misma para un PyME.
P04.2 – Comité Estratégico de TI P04.3 – Comité Directivo de TI	- La creación de un comité específico para gestionar la estrategia de TI representa un costo excesivo para las posibilidades de un PyME. Esta tarea queda habitualmente a cargo del comité (o grupo) que dirige las actividades de TI.

TABLA 7. MAPEO DE PROCESOS DE VALIT QUE APLICAN AL MODELO

Procesos o Actividades definidas por ValIT	Ubicación en la matriz de atributos	Justificación
VG1 - Garantizar liderazgo informado y comprometido	Toma de Decisiones Nivel 4 ítem a.	Proceso Gobierno de Valor: VG.
VG2 - Definir e implementar procesos.	Estructura de TI de Nivel 4 ítem b. Valor de TI Nivel 4 ítems a y d. Valor de TI Nivel 5 ítems a y c.	
VG3 - Definir roles y responsabilidades.	Estructura de TI de Nivel 4 ítems a y b.	
VG4 - Garantizar responsabilidad apropiada y aceptada.	Estructura de TI de Nivel 4 ítems a y b.	
VG5-Definir necesidades de información.	Servicios de TI de Nivel 4 ítems a, b y c.	
VG6- Establecer necesidades de informes	Valor de TI de Nivel 4 ítems a y c. Servicios de TI de Nivel 4 ítems a, b, y c. Seguridad de TI Nivel 4 ítem a.	

	Toma de decisiones de Nivel 4 ítem a.	
	Gobierno de TI, tem c.	

TABLA 8. MAPEO DE PROCESOS DE VALIT QUE NO APLICAN AL MODELO

Proceso y Práctica	Justificación
VG7 - Establecer estructuras organizativas.	No aplica a la realidad de las pymes en Uruguay porque estas no cuentan con los RRHH ni económicos requeridos para implementar las estructuras que define este proceso, que es muy amplio, detallista y difícilmente tercerizable debido al grado de conocimiento que requiere de la organización.
PM7 - Evaluar el caso de negocio del concepto de programa inicial.	No aplica a la realidad de las pymes en Uruguay porque estas no cuentan con los RRHH ni económicos requeridos para implementar este proceso que es muy amplio, detallista y difícilmente tercerizable debido al grado de conocimiento que requiere de la organización.
PM8 - Evaluar y asignar una puntuación relativa al caso de negocio del programa	No aplica a la realidad de las pymes en Uruguay porque estas no cuentan con los RRHH ni económicos requeridos para implementar este proceso que es muy amplio, detallista y difícilmente tercerizable debido al grado de conocimiento que requiere de la organización.
IM3 - Adquirir un claro entendimiento de los programas candidatos.	No aplica a la realidad de las pymes en Uruguay porque estas no cuentan con los RRHH ni económicos requeridos para implementar este proceso amplio y detallista.
IM8 - Desarrollar un caso de negocio detallado del programa.	No aplica a la realidad de las pymes en Uruguay porque estas no cuentan con los RRHH ni económicos requeridos para implementar este proceso amplio y detallista.

X. ANÁLISIS DE LOS NIVELES DE MADUREZ DE LAS PYMES

La clasificación de las PyMEs utilizando el modelo de madurez propuesto muestra claramente que dos de cada tres organizaciones están en un nivel muy bajo de madurez (entre los niveles 1 y 2) tal como podemos apreciar en la tabla 9. Es oportuno recordar que en modelo presentado, la admisión en un nivel es estricta, es decir que deben cumplirse todos los atributos de un determinado nivel para calificar como perteneciente al mismo.

TABLA 9.DISTRIBUCIÓN DE ORGANIZACIONES POR NIVEL DE MADUREZ

Nivel	Cantidad de Empresas	Porcentaje del total
1	4	13%
2	16	53%
3	8	27%
4	2	7%
5	0	0%

El 53% de las empresas estudiadas se encuentra en un nivel 2 de madurez, un 27% en un nivel 3, un 13% en un nivel 1, un 7% en un nivel 4 y no hay empresas que tengan un nivel 5 de madurez tal como los podemos apreciar en la tabla 9 y en la figura 6.

Se puede observar en la tabla 2 y la en la figura 6 que un 53% de las empresas estudiadas se encuentra en un nivel 2 de madurez, un 27% en un nivel 3, un 13% en un nivel 1, un 7% en un nivel 4 y no hay empresas que tengan un nivel 5 de madurez.



Figura 6. Gráfica con distribución de empresas por nivel de madurez

Al analizar la distribución de pequeñas y medianas empresas en relación a los distintos niveles de madurez se puede observar en la figura 7 que en los niveles 1,2 y 3 hay empresas pequeñas y medianas siendo mayor el número de las últimas. Es importante destacar que para el nivel 4 de madurez todas las empresas son medianas.

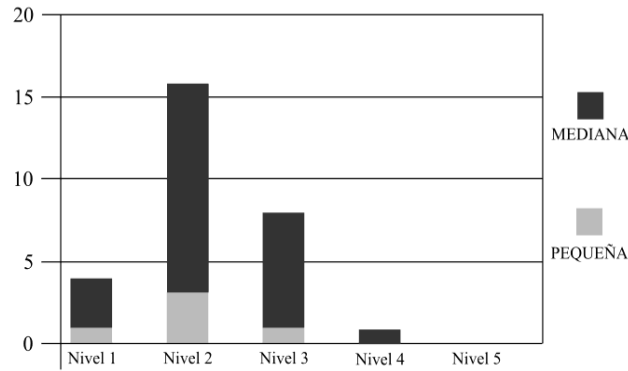


Figura 7. Gráfica comparativa de las pequeñas y medianas empresas por nivel.

En relación al número de empleados de TI podemos apreciar en la figura 8 que en nivel 1 de madurez todas las empresas tienen hasta 5 empleados de TI, a diferencia del nivel 4 de madurez donde no existen empresas con menos de 5 empleados de TI, siendo el número de empleados de TI entre 6 y 20. En el nivel 2 y 3 de madurez podemos ver que la mayoría de las empresas tienen hasta 5 empleados de TI, un 70% para nivel 2 y un 63% para nivel 3, existiendo algunas empresas con un número mayor a 5 empleados, siendo mayor este número para el nivel 3.

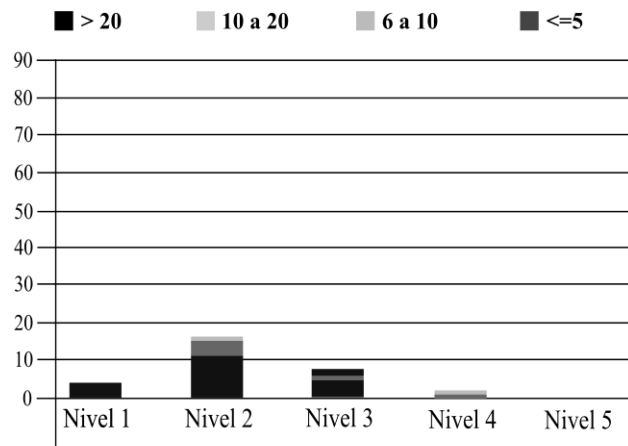


Figura 8. Gráfica comparativa de la cantidad de empleados de TI por nivel

Si se analiza la distribución de las distintas industrias a la que pertenecen las organizaciones en los distintos niveles de madurez se puede observar en la figura 9 que en los niveles 1,2 y 3 el porcentaje de servicios es mayor que en las demás industrias y que en el nivel 4 es igual a la industria de Telecomunicaciones/IT. Se puede apreciar que las empresas familiares pertenecen a los niveles 1,2 y 3.

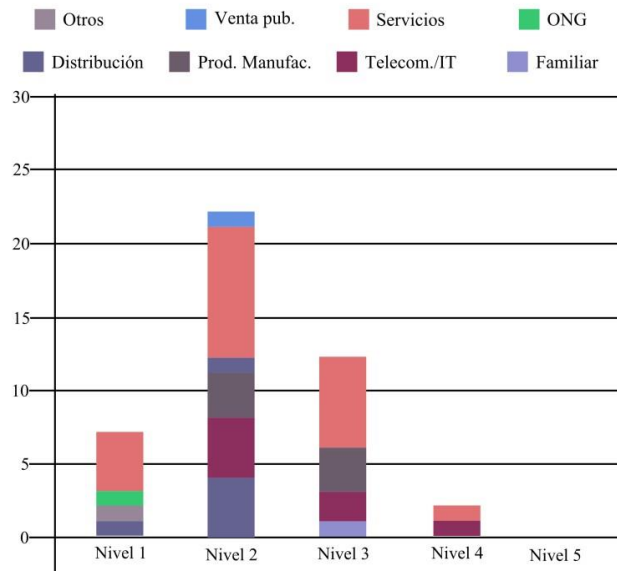


Figura 9. Gráfica comparativa por nivel.

Desde el punto de vista de la distribución de la ubicación de las organizaciones en Montevideo e Interior del Uruguay se puede observar en la figura 10 que en el nivel 1 es mayor el número de organizaciones del interior del país, en el nivel 2 es mayor el número de organizaciones de Montevideo, en el nivel 3 es muy similar el número de organizaciones de Montevideo y del interior del país, mientras que es interesante destacar que en el nivel 4 todas las organizaciones pertenecen a la capital del país.

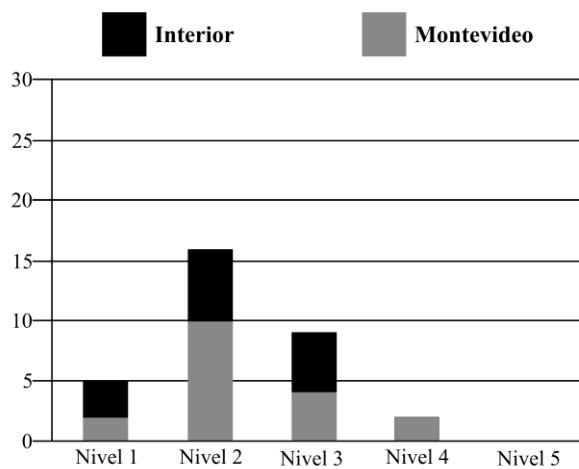


Figura 10. Gráfica comparativa de Montevideo e interior del país

XI. CONCLUSIONES Y TRABAJOS FUTUROS

Del análisis de la matriz de atributos de madurez, se desprende claramente que el esfuerzo para llevar una empresa de nivel 1 a nivel 2 es mínimo y de bajo costo. Consideramos que resulta estratégico centrar la atención en estos dos niveles de madurez ya que además de ser los más inmaduros son los que agrupan a la mayoría de las empresas (Tabla 8).

Alcanza con aplicar algunas medidas de seguridad prácticas que no implican más inversión que las de informarse en alguno de los marcos de trabajo, los que además en el caso de COBIT (IT Governance Institute, 2012) y ValIT (IT Governance Institute, 2008) son de acceso libre y gratuito. La aplicación de las buenas prácticas de estos primeros niveles es directa y no requiere de gran estructura ni de conocimiento experto.

El esfuerzo necesario para llevar a una empresa de nivel 2 al nivel 3 es ya más importante. Sin embargo la implementación de los cambios necesarios no implica grandes costos, sino más bien un cambio de cultura organizacional donde se asigne a TI un rol de importancia como herramienta para la consecución de los objetivos organizacionales. Este cambio implica que la dirección de la organización tenga conocimiento de la existencia y ventajas de la aplicación de un marco de buenas prácticas de TI, y se involucre en la difusión y aplicación de las mismas dentro de la organización.

Una PYME debiera ser capaz de implementar los cambios necesarios, definir los procesos y las estructuras necesarias de soporte de esos procesos, para aplicar el conjunto mínimo de buenas prácticas requerido por el nivel 3 de madurez en un plazo de 12 meses, sin mayores inconvenientes. Las buenas prácticas requeridas por el nivel 3 no implican conocimientos expertos en Gobernanza de TI, ni inversiones significativas en herramientas de software, o capacitación de RRHH.

Como trabajos futuros, se analizara la incidencia que tiene la Gestión del conocimiento en las PyMEs y se estudiara como inciden estos en el modelo de madurez de manera de desarrollar una hoja de ruta para que las PyMEs puedan subir de la manera más eficiente posible de un nivel de madurez al siguiente.

REFERENCIAS

- [1] P. Weill, J. Ross, IT Governance. How top performers manage IT decision rights for superior results, in, Harvard Business School Press, Boston, Massachusetts, 2004
- [2] OCDE, Principios de Gobierno Corporativo de la OCDE, in, Organización para la cooperación y el desarrollo económicos, París, 2004.
- [3] ESADE, CorporateGovernance, el buen gobierno de la empresa, in: EGuíame!, la Caixa, 2004.
- [4] BCU, Instituciones de intermediación financiera - Normativa sobre gobierno corporativo y sistema de gestión integral de riesgos., in, 2008.
- [5] ITGI, CobiT© 4.1, in, ISACA, USA, 2007.
- [6] P. Weill, J. Ross, Four Questions Every CEO Should Ask About IT, in: The Wall Street Journal, 2011.
- [7] DINAPYME, Criterio de clasificación de Empresas en el Uruguay, in, 1995.
- [8] DINAPYME, Estructura de las Empresas PYMES en el Uruguay, in: MIEM (Ed.) Observatorio PYME Uruguay, 2005.
- [9] U. DINAPYME, Teresa Herrera & Asociados Consultoría, Encuesta Nacional de mPymes industriales y de servicios, (2008).
- [10] C. Scaronne, La informalidad en las MIPYMES de Uruguay. Análisis de los costos de la formalidad, Ministerio de Industria, Energía y Minería, Montevideo, Uruguay, 2007.
- [11] N. Malhotra, Investigación de mercado, Prentice-Hall, Georgia, 2004.
- [12] ITGI, Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, in, ISACA, USA, 2008.
- [13] ITGI, Marco de riesgos de TI. Risk IT, in, ISACA, 2009. [14] ITGI, COBIT® 5 in, ISACA, 2012.
- [15] W. Van_Grembergen, S. De_Haes, An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment, Information Systems Management, 26 (2007) 123-137.
- [16] ISO, ISO/IEC 38500:2008. Corporate Governance for Information Technology., in, ISO, 2008.
- [17] A. Calder, The IT Governance Toolkit-v05, in, IT Governance Publishing, 2008.
- [18] C. Symons, IT Governance Framework. Structures, Processes, And Communication, in: C.S.-. Forrester (Ed.), 2005.
- [19] I. Terán, Inversión en TI: Un partner cada vez más importante para la PYME Latinoamericana, in: InfoWeek, 2009.
- [20] Fundatec, Análisis sectorial de implantación de las TIC en la pyme española, in: I.P. 2008 (Ed.), 2008.

- [21] A.J. Arroyo, J.D. Carrillo, The status of IT Governance in Spanish organizations. Analysis and conclusions for identifying best practices, in, 2009.
- [22] M. Bunge, La Ciencia Su Metodo Y Su Filosofia, Eudeba, Buenos Aires, 1960.
- [23] E.B. Sánchez, La investigación científica: Teoría y metodología, in, Zacatecas, 2003.

ANEXO IV - Encuesta sobre Alineamiento Estratégico de TI en las PyMEs de Uruguay

Montevideo, Uruguay

Setiembre de 2010

Contenido

1. La empresa
2. Alineamiento de TI con la estrategia de la empresa
3. Aportación de valor
4. Seguridad
5. Internet
6. Toma de decisiones
7. Gobierno de las TI
8. Conocimiento de herramientas y organizaciones de gobernanza de TI

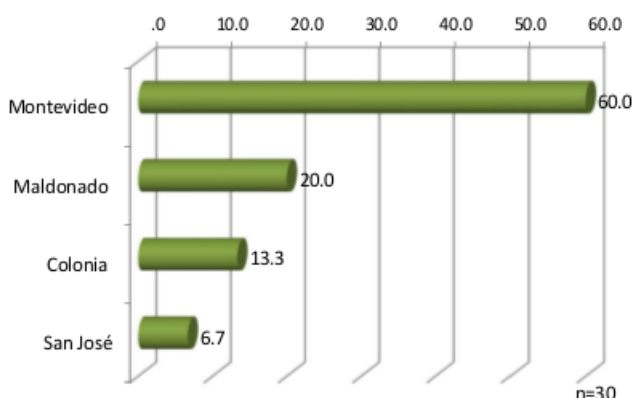
1. LA EMPRESA

1.1.1 Dimensión y estructura de la empresa

Rubro y departamento donde se ubica la empresa.

Rubro de la empresa	% de casos
Servicio de TI	16,7
Educación en gastronomía	16,7
Servicio de mecánica automotriz	6,7
Esterilizaciones de materiales médicos	6,7
Andamio y estructura	3,3
Medicina deportiva	3,3
Servicio de telefonía celular	3,3
Fabricación e importación de productos de limpieza.	3,3
Procesamiento de cuero para la industria automotriz	3,3
Hotelería	3,3
Mayorista en computación	3,3
Análisis clínico	3,3
Seguridad	3,3
Productos lacteos	3,3
Vitivinicultura	3,3
Diseño gráfico-publicidad	3,3
Fábrica de gases	3,3
Alimentación balanceada para nutrición animal	3,3
Bazar	3,3
Consultoría en costos y eficiencia energética	3,3

Gráfica 1. Departamento donde se ubica la empresa



El 16.7% de las empresas pertenecen al rubro servicio de TI y a educación en gastronomía.
El 6,7% se encuentra en el rubro de servicio de mecánica automotriz y esterilizaciones de materiales médicos.

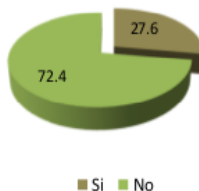
Respecto a el departamento donde se ubican las empresas, más de la mitad se encuentra en Montevidео.

1.1.2 Dimensión y estructura de la empresa

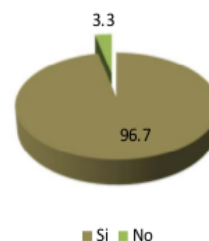
Cantidad de sucursales de la empresa, exportación y mercado interno.

Cantidad de sucursales	
Sucursales	% de casos
0	64,3
1	10,7
2	21,4
3	3,6

Gráfica 2. Exportación



Gráfica 3. Mercado Interno



El 64,3% de las empresas se caracteriza por no tener sucursales. Por su parte el 10,7% tiene una sola sucursal y el 21,4% de las empresas tiene 2. El promedio de sucursales de las empresas es de 0,64 y la mediana es 0.

Respecto aquellas empresas que exportan, puede verse que el 72,4% no lo hacen, mientras que el 27,6% si tiene como actividad la exportación.

Esta tendencia también puede verse en la gráfica n°3, donde casi el 100% de las empresas trabaja con el mercado interno.

1.1.3 Dimensión y estructura de la empresa

Cantidad de empleados.

Cantidad de empleados	
Empleados	% de casos
35	10,0
45	10,0
12	6,7
25	6,7
38	6,7
50	6,7
90	6,7
5	3,3
10	3,3
18	3,3
20	3,3
21	3,3
24	3,3
30	3,3
36	3,3
40	3,3
43	3,3
64	3,3
84	3,3
88	3,3
99	3,3

Respecto a la cantidad de empleados, puede verse que el 10% de las empresas tienen 35 y 45 empleados.

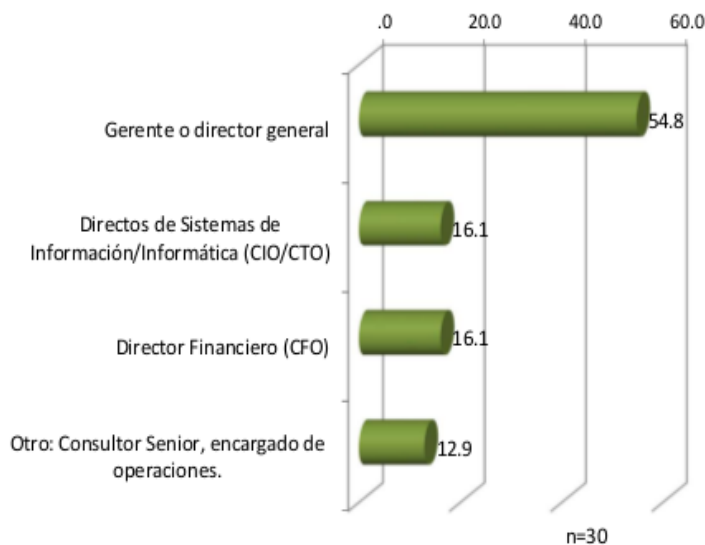
El 6,7% se caracteriza por tener 12, 25, 38, 50 y 90 empleados contratados.

La media de empleados por empresa es de 50 y la mediana se ubica en 37.

1.2 Puesto en la empresa

¿Cuál es su puesto en la empresa?

Gráfica 4. Puesto que ocupa en la empresa



Casi el 55% de los entrevistados, expresaron ocupar el lugar de gerente o director general, mientras que el 16,1% son directos de sistemas de información/informática.

El 16,1% es director financiero y el restante 12,9% es consultor senior o encargado de operaciones.

1.3. Industria a la que pertenece la organización

¿En qué industria encuadra a su organización?

Industria	% de casos
Servicios	41,3%
Telecomunicaciones/IT	17,4%
Empresa Familiar	15,2%
Producción de bienes manufacturados	13%
Producción materias primas	4,3%
Distribución	4,3%
ONG	4,3%

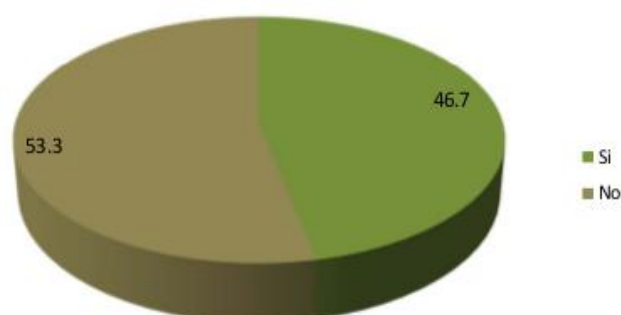
El 41,3% de las empresas se caracterizan por dedicarse al sector servicio. El 17,4% se enmarca en las telecomunicaciones/IT y el 15,2% son empresas familiares.

Por su parte, el 13% de las organizaciones se dedican a la producción de bienes manufacturados.

1.4.1 Dimensión y estructura de TI en la empresa

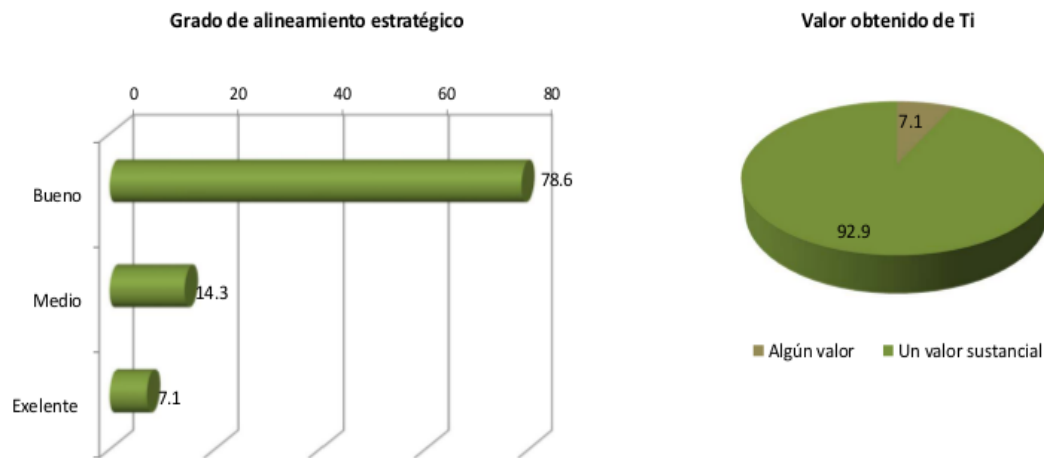
¿Existe una estructura de TI definida en la empresa?

Gráfica 5. Existencia de una estructura definida de TI



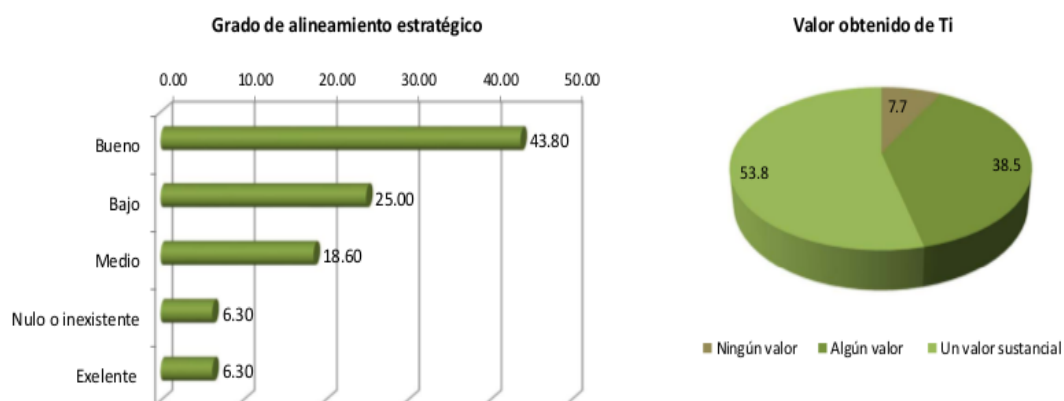
El 46,7% de las empresas tiene una estructura definida de TI, mientras que el 53,3 % no la tiene.

1.4.1.1 Empresas con infraestructura de Ti en relación al grado de alineamiento estratégico y la entrega de valor de Ti



Analizando las empresas **que tienen una infraestructura de TI en relación al grado de alineamiento estratégico**, puede verse que el 78% lo evalúa como bueno y el 14% entiende que es medio. Si se analiza las **empresas que cuentan con infraestructura según el valor obtenido de TI**, se observa que el 92% considera que esta obteniendo un valor sustancial de TI y el 7% expresa que obtiene algún valor de TI en su organización.

1.4.1.2 Empresas que no cuentan con infraestructura de Ti en relación al grado de alineamiento estratégico y la entrega de valor de Ti



Analizando las empresas **que no tienen una infraestructura de TI en relación al grado de alineamiento estratégico**, puede verse que el 43% lo evalúa como bueno y el 25% entiende que es bajo. Si se analiza las **empresas que cuentan con infraestructura según el valor obtenido de TI**, se observa que el 54% considera que esta obteniendo un valor sustancial de TI, el 38% expresa que obtiene algún valor de TI en su organización y el restante 7% entiende que no obtiene ningún valor de TI.

1.4.2 Dimensión y estructura de TI en la empresa

Cantidad de empleados

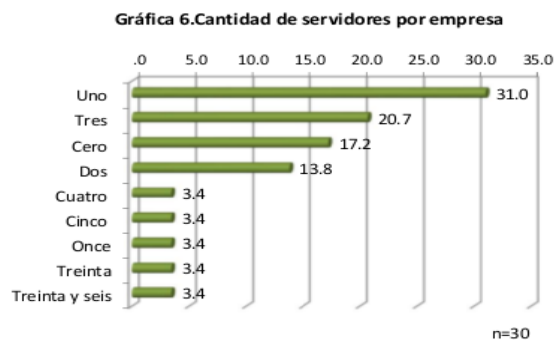
Cant_empleados	% de casos
1	26,7
5	16,7
0	10,0
3	10,0
4	10,0
2	6,7
6	3,3
8	3,3
10	3,3
20	3,3
28	3,3
100	3,3

En el total, el promedio de empleados por empresa es de 7,67, mientras que el valor de la mediana de empleados es 3.
 El 26,7% de las empresas se caracteriza por tener solo un empleado, el 16,7% tiene 5 empleados a cargo.
 Por otra parte, hay que destacar que son pocos los casos de las empresas que tienen un alto número de empleados.

1.4.3 Dimensión y estructura de TI en la empresa

Cantidad de PC y cantidad de servidores

Cant_PC	% de casos
5	10,0
6	3,3
8	3,3
9	6,7
10	13,3
13	3,3
15	6,7
16	3,3
17	6,7
19	3,3
20	3,3
25	3,3
30	10,0
36	3,3
40	3,3
50	3,3
60	10,0
100	3,3

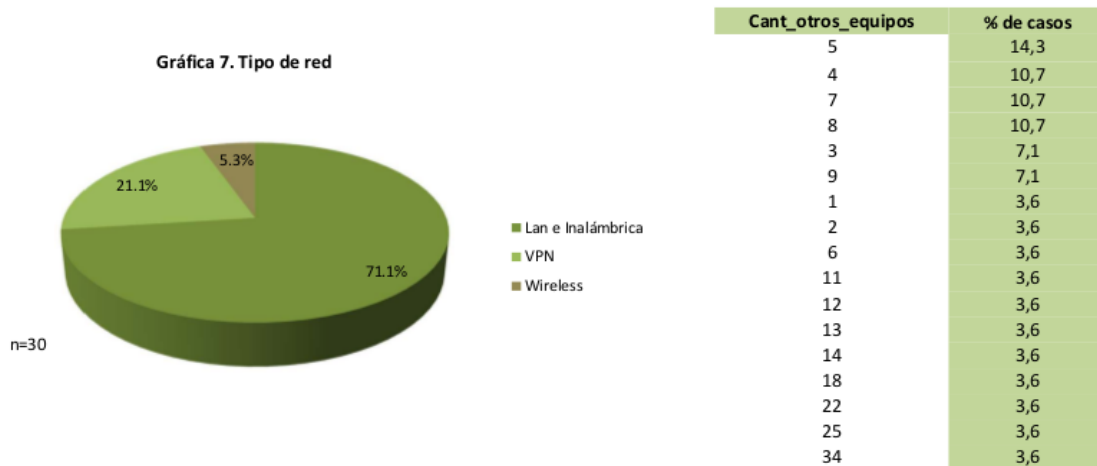


En el total, el promedio de PC por empresa es de 24,67, mientras que el valor de la mediana de 16,50.

Respecto a la **cantidad de servidores** por empresa, puede observarse que el 31% cuenta con 1 servidor, el 20,7% tiene 3 y el 17,2% se caracteriza por no tener servidores en la empresa. La media de servidores por empresa es de 4,17, y la mediana se ubica en 2.

1.4.4 Dimensión y estructura de TI en la empresa

Tipo de red y cantidad de otros equipos

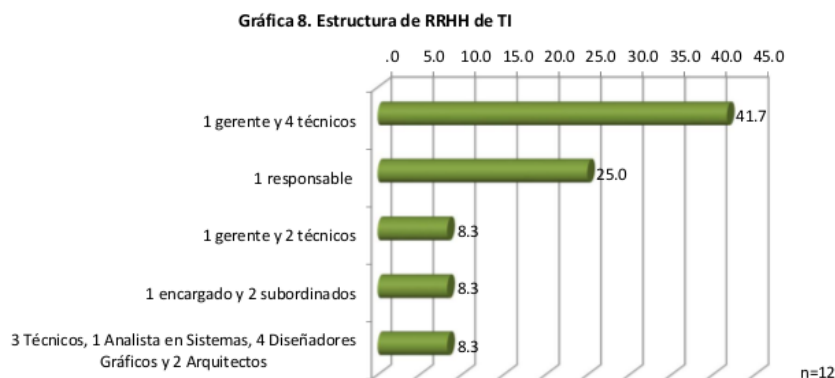


El tipo de red que más utilizan las empresas es LAN e Inalámbrica (71%) y el segundo tipo de red más usada es VPN con un 21,1%.

Respecto a la cantidad de otros equipos, el 14,3% de las empresas tiene 5 y el 10,7% tiene 4, 7 y 8 equipos. En promedio, las empresas utilizan 9,25 equipos para trabajar. En el caso de la mediana, esta se ubica en 7.

1.4.5 Dimensión y estructura de TI en la empresa

Roles en la estructura de RRHH de TI



Respecto a la estructura de RRHH de TI, es importante notar que solo 12 de las 30 empresas entrevistadas tienen una estructura definida.

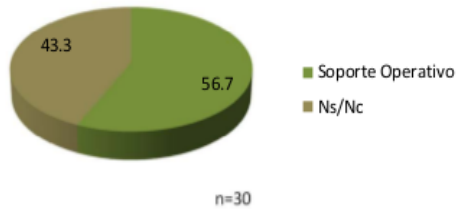
De estas empresas, el 41,7% se caracteriza por tener 1 gerente y 4 técnicos. Cabe adarar que estos técnicos son externos, es decir, terciarizados.

El 25% tiene como principal característica de la estructural de RRHH la presencia de un solo responsable.

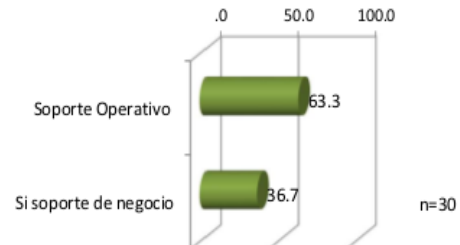
1.4.6 Dimensión y estructura de TI en la empresa

Responsabilidad de TI y soporte al negocio

Gráfica 9. Responsabilidad de TI



Gráfica 10. Soporte al negocio



Respecto a la **responsabilidad de TI**, solo un 56,7% respondió tener una responsabilidad definida, que consiste en dar un soporte operativo.

En el gráfico 10, se muestra, el soporte al negocio. Puede verse que el 36,7% tiene un soporte de negocio. El 63,3% de las empresas expreso que solo tiene un soporte operativo.

1.4.7 Dimensión y estructura de TI en la empresa

Presupuesto asignado a TI

% de presupuesto	% de casos
5	23,1
10	23,1
3	7,7
8	7,7
15	7,7
25	7,7
30	7,7
40	7,7
50	7,7

El presupuesto asignado de las empresas a TI, en promedio es de 16,58%.

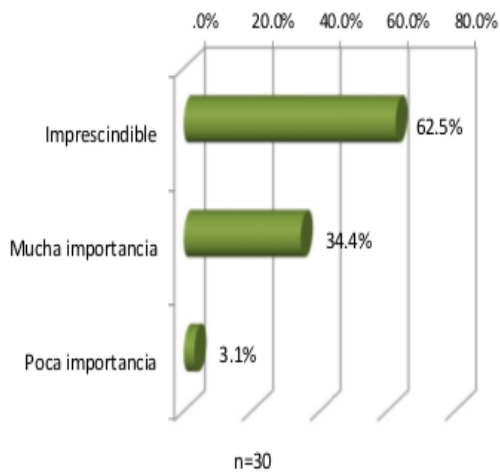
El 23,1% de las empresas asignan un 5% y un 10% de su presupuesto a TI.

Como se ve en la tabla, los presupuestos asignados a TI van desde un 3% hasta un 50% .

1.5 Importancia de TI en la organización

¿Qué importancia considera que tiene TI en la organización? ¿Por qué?

Gráfica 12. Importancia de TI en la organización

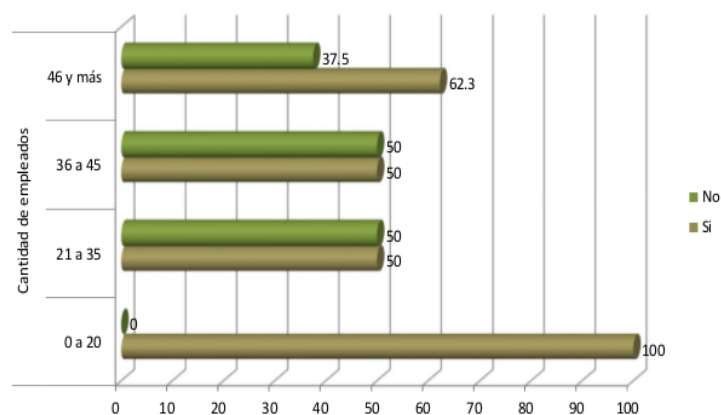


El 62,5% de las empresas considera que es imprescindible TI en la organización. El 34,4% expresa que es muy importante y solo un 3,1% de los entrevistados lo evalúa como poco importante.

Motivo de importancia	% de casos
Necesario para maximizar el resultado del negocio	25,7%
Software de gestión de empresa fue desarrollada a medida	14,3%
Sistema para la contabilidad y la facturación	11,4%
Seguridad física de la empresa	5,7%
Sistema académico	5,7%
Hosting y administración del sitio web	2,9%
Mantenimiento de PC y red local	2,9%
Trabajo de diseño industrial CAP	2,9%
O3 para mediciones, gráficas, e indicadores	2,9%
BAS para contabilidad y stock. Funciona interconectado con Panoramix	2,9%
Diversidad de criterios entre los socios directores	2,9%
Utilización de un software de datos de los pacientes en un único PC sin conexión a internet.	2,9%
Conexión con la casa matriz para upload	2,9%

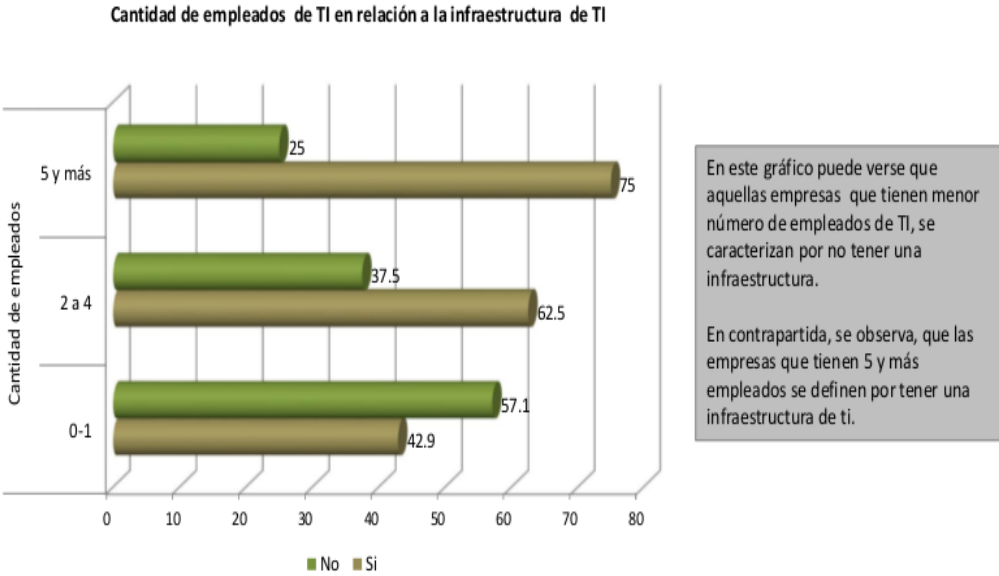
1.6 Cantidad de empleados en relación a la infraestructura de TI

Cantidad de empleados en relación a la infraestructura

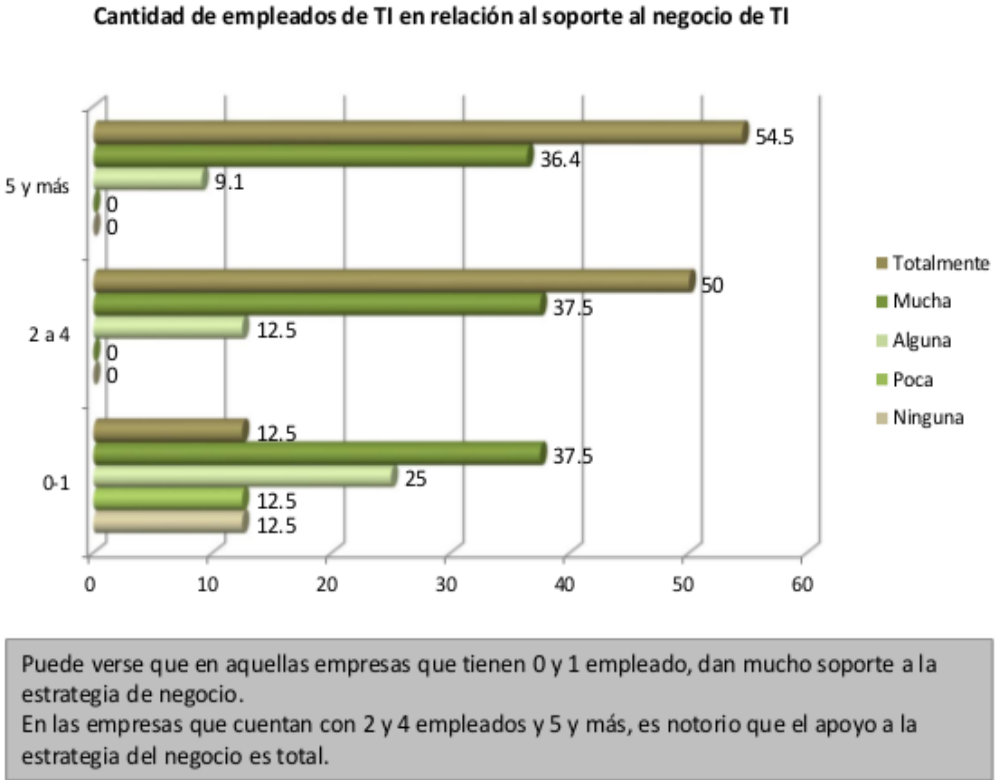


Puede verse que en el 100% de las empresas que tienen entre 0 y 20 empleados, existe una infraestructura de TI. En aquellas empresas que tienen entre 21 a 35 o 36 a 45 empleados, es característico que la mitad de las empresas tengan una infraestructura de TI y la otra mitad no. En las empresas que tienen 46 y más empleados, se observa que el 62% tiene una infraestructura de TI y el 37% se caracteriza por no tenerla.

1.7 Cantidad de empleados de TI en relación a la infraestructura de TI

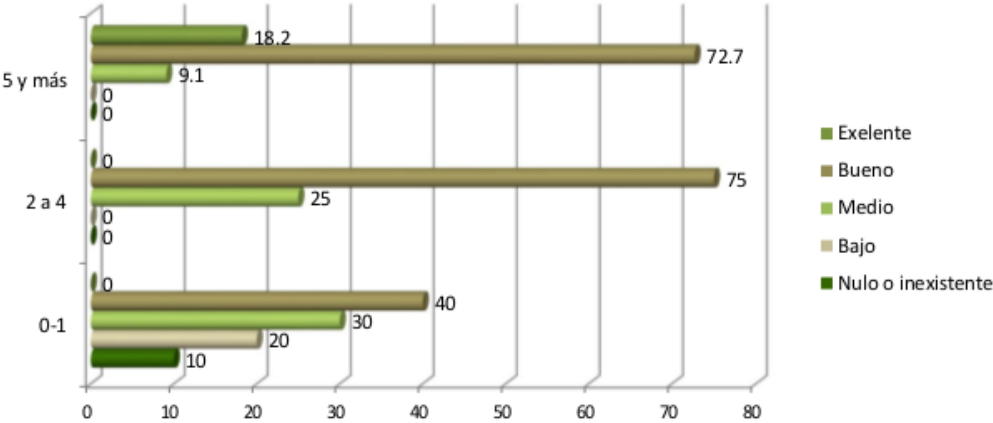


1.8 Cantidad de empleados de TI en relación al soporte al negocio de TI



1.9 Cantidad de empleados de TI en relación al grado de alineamiento de TI a los objetivos del negocio

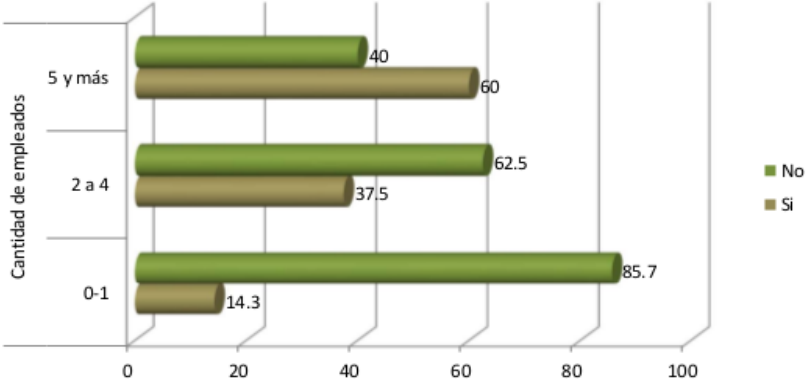
Cantidad de empleados de TI en relación al grado de alineamiento de TI



Las empresas que tienen menos cantidad de empleados, se caracterizan por evaluar como bueno y medio el grado de alineamiento de TI a los objetivos del negocio. En aquellas empresas de 5 y más empleados, conciben el grado de alineamiento como bueno para el 72% y exelente para el 18% de los entrevistados.

1.9.1 Cantidad de empleados de TI en relación al grado de aportación de valor de TI

Cantidad de empleados de TI en relación al grado de aportación de TI



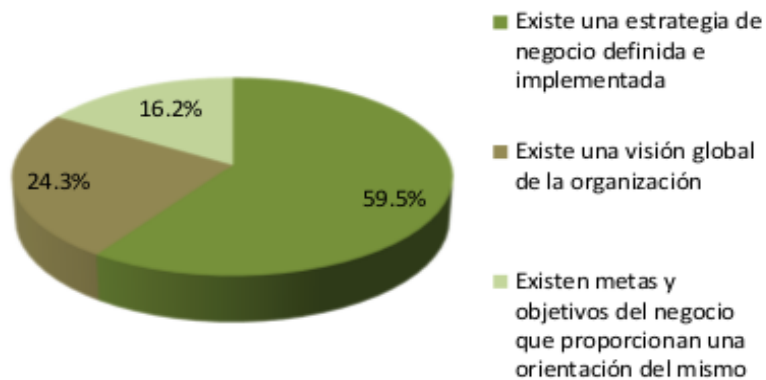
En las empresas que tienen 0-1 empleado, se caracterizan notoriamente por no medir la aportación de TI al negocio. En oposición, se observa que las empresas que tienen 5 y más empleados, son quienes miden mayormente el grado de aportación, ya que el 60% expresa que lo hace y el 40% no lo mide.

2. ALINEAMIENTO DE TI CON LA ESTRATEGIA DE LA EMPRESA

2.1 Existencia de una estrategia de negocio definida o disposición de una visión global

Su organización ¿tiene una estrategia de negocio definida o dispone de una visión global?

Gráfica 13. Existencia de estrategia definida o disposición de una visión global

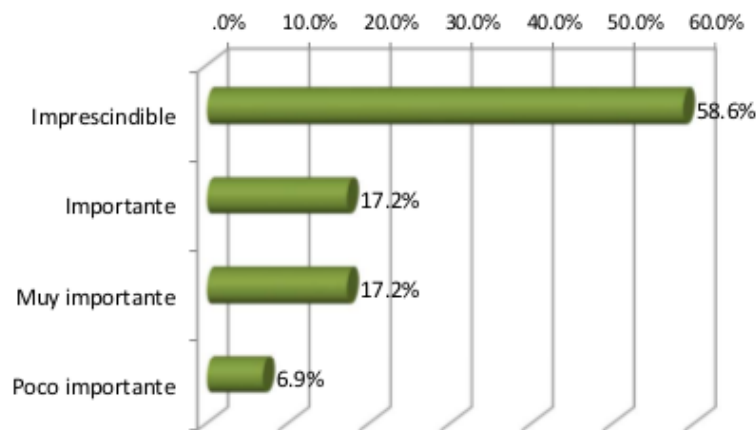


Casi el 60% de los entrevistados, expresa que existe en su empresa una estrategia de negocio definida e implementada. El 24,3% explica que existe una visión global de la organización y el restante 16,2% entiende que existen metas y objetivos del negocio que proporcionan una orientación del mismo.

2.2 Importancia de TI como elemento que permite la consecución de una estrategia o visión

Teniendo en cuenta la estrategia de negocio o la visión global de la organización, ¿qué importancia concede a las TI como elemento que permite la consecución de una estrategia o visión?

Gráfica 14. Importancia de TI

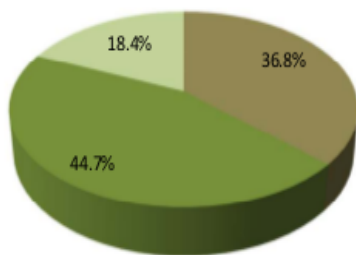


Casi el 60% de los entrevistados, expresa que es imprescindible TI como elemento que permite la consecución de una estrategia o visión. El 17,2% entiende que TI es un elemento muy importante e importante para dicha consecución y el restante 6,9% lo evalúa como poco importante.

2.3 Filosofía de TI en su empresa

Con respecto a las TI, ¿cómo describiría la filosofía de TI en su empresa?

Gráfica 15. Filosofía de TI en su empresa



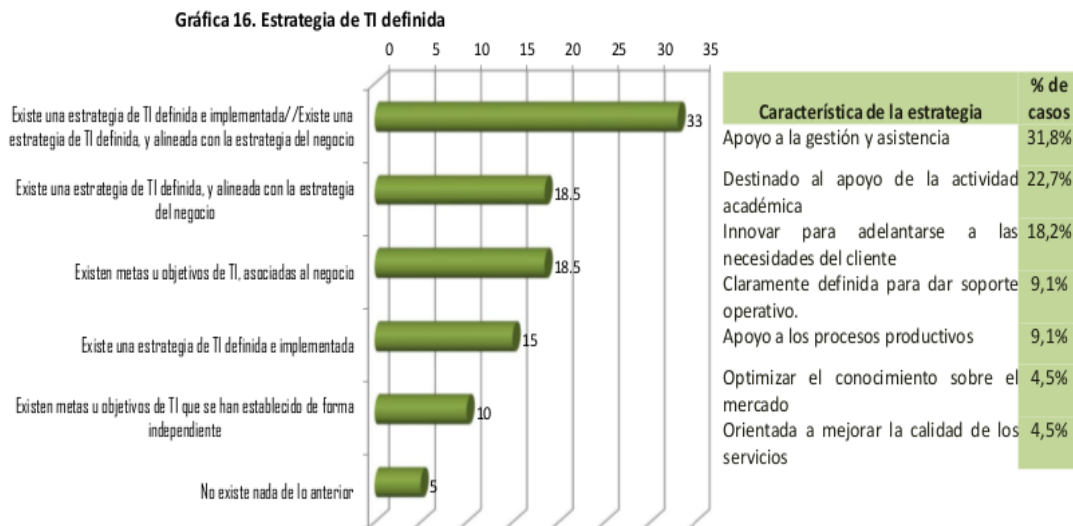
- Innovación (uso de las TI como arma competitiva)
- Funcional (inversiones en tecnologías líderes, pero de apoyo al negocio, principalmente)
- Conservadora (inversiones en tecnologías maduras, probadas)

Filosofía de TI en categorías	% de respuesta
Innovación/Funcional	40,8
Funcional/ Conservadora	31,6
Innovación/Conservadora	27,6

El 45% de las empresas tiene una filosofía de TI en su empresa funcional, el 36,8% se caracteriza por tener una filosofía de innovación y el restante 18,4% es conservadora, es decir, que invierten en tecnologías maduras y probadas.

2.4 y 2.5 Estrategia de TI definida

Su organización, ¿tiene una estrategia de TI definida?

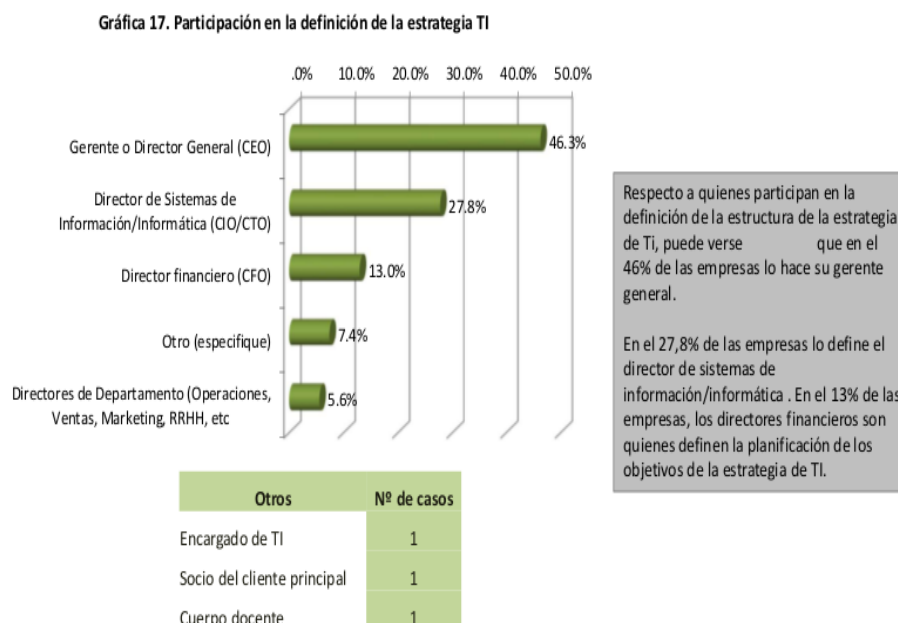


Respecto a la estrategia de TI definida, en el 33 % de las empresas existe conjuntamente una estrategia definida de TI e implementada y una estrategia definida y alineada con la estrategia del negocio.

Para la el 31,8% de los entrevistados, la estrategia de TI tiene como principal característica que es de apoyo a la gestión y de asistencia.

2.6 Participación en la planificación de la estrategia de TI

Si existe una estrategia y planificación de TI, ¿Quiénes participan de la definición de procesos, estructuras, y de la planificación de sus objetivos?



2.6 .1 Participación en la planificación de la estrategia de TI

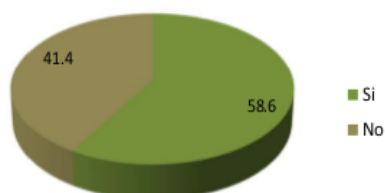
Si existe una estrategia y planificación de TI, ¿Quiénes participan de la definición de procesos, estructuras, y de la planificación de sus objetivos?

Agrupación en categorías de quienes participantes en la planificación de la estrategia de TI	% de respuesta
Gerente o Director General (CEO)// Director de Sistemas de Información-Informática (CIO/CTO)//Director financiero (CFO)	33,3
Gerente o Director General (CEO)// Director de Sistemas de Información-Informática (CIO/CTO)	28,4
Gerente o Director General (CEO)// Director financiero (CFO)	22,7
Director de Sistemas de Información-Informática (CIO/CTO)//Director financiero (CFO)	15,6

2.7 Existencia de una estructura de TI definida

Si existe una estrategia y planificación de TI ¿Existe una estructura definida?, ¿y qué arquitectura tiene?

Gráfica 18. Existencia de estructura definida



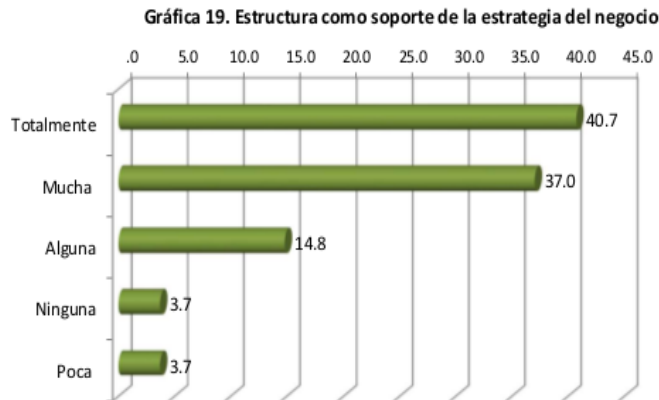
Característica de la estructura-arquitectura	% de casos
Se busca la simplicidad y la calidad en el acceso de los usuarios a los servicios	35,3
Se prioriza la eficiencia en la gestión	35,3
Da soporte a una estructura de 85 PCs sobre una LAN (UTP), con sistemas integrados corporativos	11,8
La arquitectura es centralizada y descentralizada	5,9
Apoya a los procesos productivos	5,9
Orientada al servicio post-venta	5,9

El 58% de las empresas tiene una estructura definida, mientras que el 41,4% expresa no tenerla.

Las dos características que más se destacan respecto a la estructura consisten en buscar la simplicidad y calidad en el acceso de los usuarios a los servicios y priorizar la eficiencia en la gestión.

2.8 Arquitectura y estructura como soporte o apoyo de la estrategia del negocio

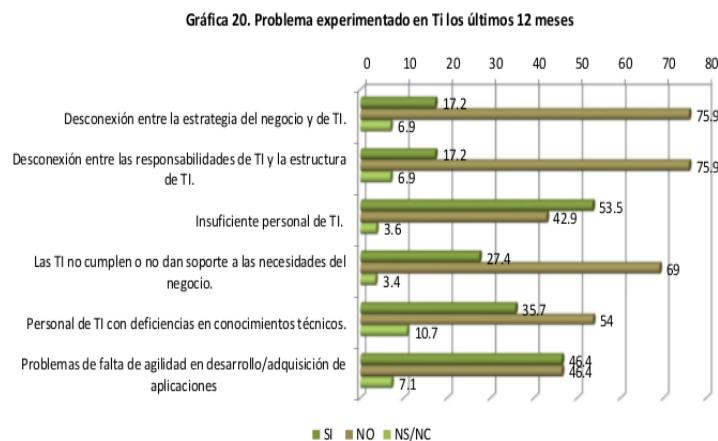
Si existe una estrategia y planificación de TI, ¿en qué medida cree Ud. que las estructuras y arquitectura existentes soportan o apoyan la estrategia del negocio?



El 40% de los entrevistados cree que la estructura y la arquitectura soportan totalmente la estrategia del negocio. Para el 37% la arquitectura apoya mucha la estrategia y para el 14,8% el soporte es alguno. Por último, para el 3,7% de las empresas la arquitectura tiene poco o ningún apoyo en la estrategia del negocio.

2.9 Problemas experimentados en las TI los últimos 12 meses

¿Cuál de los siguientes problemas ha experimentado en las TI los últimos 12 meses?



El problema más frecuente que se ha experimentado en los últimos 12 meses, con un 60,7% de las empresas entrevistadas es la inexistencia de indicadores de eficiencia de TI. El segundo problema más frecuente es la inexistencia de procesos de revisión y evaluación de los indicadores y objetivos de TI. Para un 53,5% de los entrevistados, los problemas experimentados tienen que ver con la insuficiencia de personal de TI. En cuarto lugar, el problema refiere a la inexistencia de un plan de Continuidad del Negocio. Finalmente en último lugar se encuentran problemas relacionados con la inexistencia de indicadores de calidad de servicios TI y problemas por falta de agilidad de desarrollo/adquisición de aplicaciones.

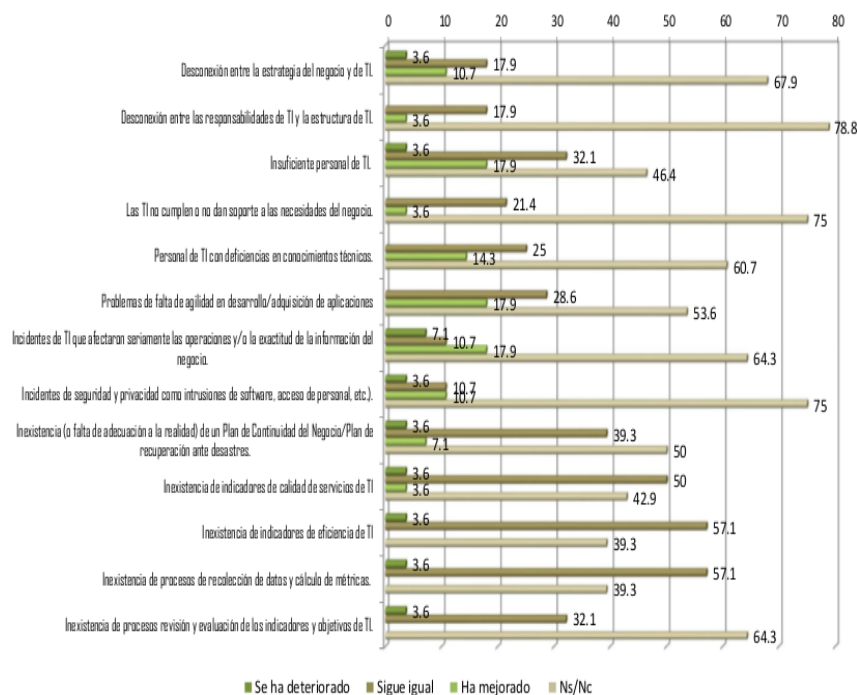
2.10 Importancia de los problemas

¿Qué importancia tuvieron esos problemas?

Problema	Mucha	Bastante	Alguna	Poca	Ninguna	Ns/Nc
Desconexión entre la estrategia del negocio y de TI.	14,3	3,6	3,6		7,1	71,4
Desconexión entre las responsabilidades de TI y la estructura de TI.		35,7	10,7	3,6	3,6	46,4
Insuficiente personal de TI.		35,7	10,7	3,6	3,6	46,4
Las TI no cumplen o no dan soporte a las necesidades del negocio.	3,6	11	10,7		3,6	71,4
Personal de TI con deficiencias en conocimientos técnicos.		21	7,1	3,6	3,6	64,3
Problemas de falta de agilidad en desarrollo/adquisición de aplicaciones	3,6	32,1	7,1	3,6	3,6	64,3
Incidentes de TI que afectaron seriamente las operaciones y/o la exactitud de la información del negocio.	25	3,6		3,6	3,6	64,3
Incidentes de seguridad y privacidad como intrusiones de software, acceso de personal, etc.).	3,6	3,6	3,6		7,1	82,1
Inexistencia (o falta de adecuación a la realidad) de un Plan de Continuidad del Negocio/Plan de recuperación ante desastres.	3,6	28,6	10,7		10,7	46,4
Inexistencia de indicadores de calidad de servicios de TI	3,6	17,9	21,4	7,1	7,1	42,9
Inexistencia de indicadores de eficiencia de TI	3,6	17,9	25	7,1	7,1	39,3
Inexistencia de procesos de recolección de datos y cálculo de métricas.	3,6	17,9	25	7,1	7,1	39,3
Inexistencia de procesos revisión y evaluación de los indicadores y objetivos de TI.	3,7	10,7	7,1	7,1	7,1	64,3

2.11 Situación de los problemas respecto a los últimos 12 meses

Para los problemas anteriores, ¿cree que la situación, con respecto a los últimos doce meses, se ha deteriorado, ha mejorado o continúa igual?



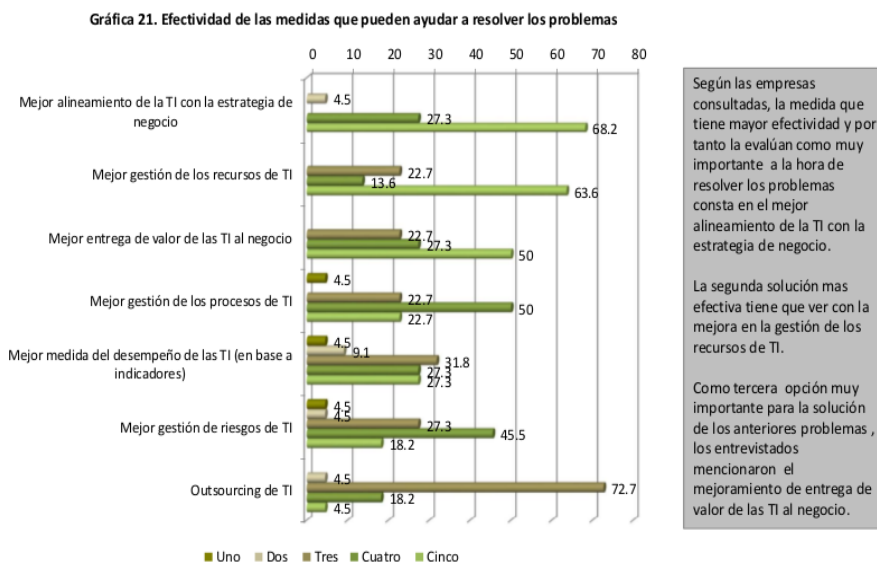
2.12 Grado de urgencia que deberían tratarse estos problemas en los doce próximos meses

Para los problemas anteriores, ¿cree que la situación, con respecto a los últimos doce meses, se ha deteriorado, ha mejorado o continúa igual?

Problema	Mucha	Bastante	Media	Poca	Ninguna	Ns/Nc
Desconexión entre la estrategia del negocio y de TI.	13,8		3,4		6,9	75,9
Desconexión entre las responsabilidades de TI y la estructura de TI.		6,9	3,4		6,9	82,8
Insuficiente personal de TI.	3,4	31	10,3		3,4	51,7
Las TI no cumplen o no dan soporte a las necesidades del negocio.	10,3	3	3,4	3,4	3,4	75,9
Personal de TI con deficiencias en conocimientos técnicos.		21	6,9		3,4	69
Problemas de falta de agilidad en desarrollo/adquisición de aplicaciones	10,3	24,1	10,3			55,2
Incidentes de TI que afectaron seriamente las operaciones y/o la exactitud de la información del negocio.	17,2	10,3	3,4		3,4	65,5
Incidentes de seguridad y privacidad como intrusiones de software, acceso de personal, etc.).	3,4		3,4	3,4	3,4	86,2
Inexistencia (o falta de adecuación a la realidad) de un Plan de Continuidad del Negocio/Plan de recuperación ante desastres.	10,3	17,2	10,3	3,4	3,4	55,2
Inexistencia de indicadores de calidad de servicios de TI	3,4	20,7	24,1		6,9	44,8
Inexistencia de indicadores de eficiencia de TI		24,1	27,7		6,9	41,4
Inexistencia de procesos de recolección de datos y cálculo de métricas.		24,1	27,6		6,9	41,4
Inexistencia de procesos revisión y evaluación de los indicadores y objetivos de TI.		17,2	10,3		6,9	65,5

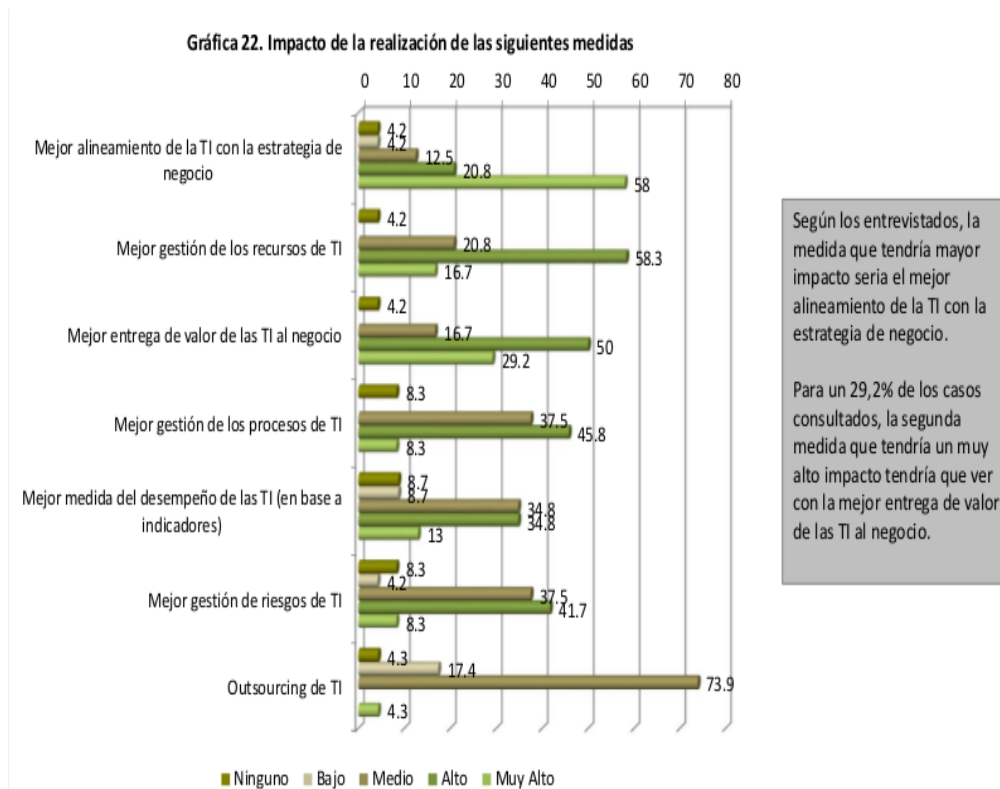
2.13 Efectividad de las siguientes medidas de alto nivel que pueden ayudar a resolver estos problemas

Valore con qué efectividad las siguientes medidas de alto nivel pueden ayudarle a resolver estos problemas. Use la escala 1 – 5, donde 1 es “nada importante” y 5 es “muy importante”.



2.14 Valoración del impacto que tendría la realización de las siguientes medidas en la organización

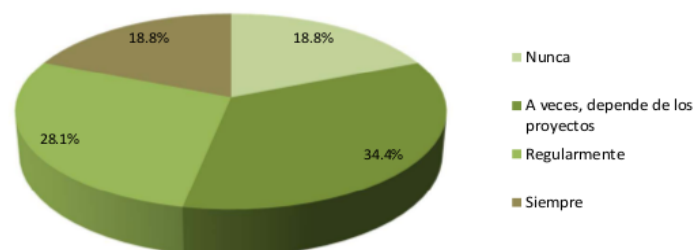
Igualmente, valore qué impacto tendría la realización de las siguientes medidas en su organización.



2.15 Periodicidad que informa su departamento de TI al negocio sobre potenciales oportunidades

¿Con qué periodicidad informa su departamento de TI al negocio sobre potenciales oportunidades de negocio que están asociadas a nuevas tecnologías?

Gráfica 23. Periodicidad que informa su departamento de TI al negocio sobre potenciales oportunidades

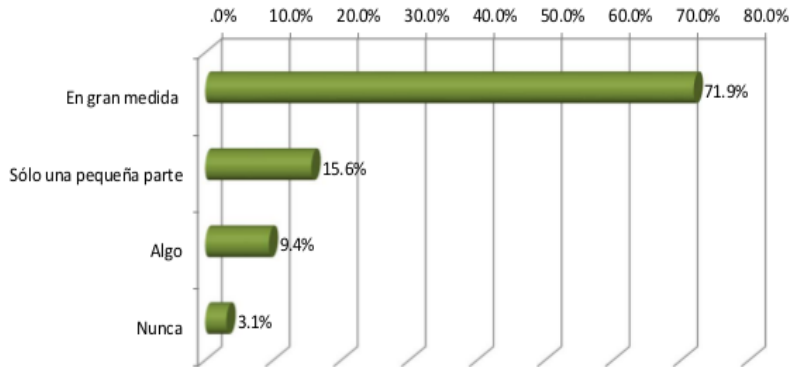


El 34,4% de las empresas consultadas, entiende que la periodicidad con que se informa depende de los proyectos. El 28,1% expresa que su departamento de TI informa regularmente al negocio sobre potenciales oportunidades de negocio que están asociadas a nuevas tecnologías. Según el 18,8% siempre se informa al negocio sobre oportunidades y el restante 18,8% establece que su departamento de TI nunca informa al negocio.

2.16 Profundidad de comprensión de las necesidades de los usuarios

¿En qué profundidad su departamento de TI comprende las necesidades de los usuarios?

Gráfica 24. Profundidad de la comprensión de las necesidades de los usuarios

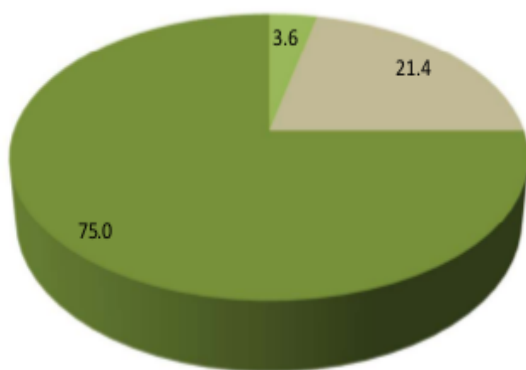


El 71,9% de los departamentos de TI comprende en gran medida las necesidades de los usuarios, en cambio el 15,6% entiende que la comprensión es una pequeña parte.

2.17 Departamento de TI como soporte a las necesidades de los usuarios

¿En qué medida su departamento de TI da soporte a las necesidades de los usuarios?

Gráfica 25. Soporte a las necesidades de los usuarios



■ En ninguna ■ En alguna medida ■ En gran medida

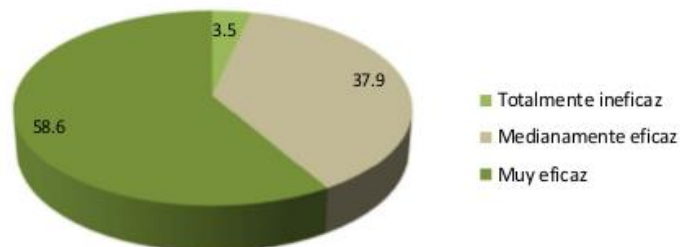
El 75% de los departamentos de TI da soporte a las necesidades de los usuarios.

El 21,4% da soporte en alguna medida y el restante 3,6% explica que su departamento de TI no da ningún soporte a las necesidades de los usuarios.

2.18 Eficacia de TI en cuanto a la solución de problemas de información

¿Cómo considera la eficacia de TI en cuanto a la solución de problemas de información?

Gráfica 26. Eficacia de TI en cuanto a la solución de problemas

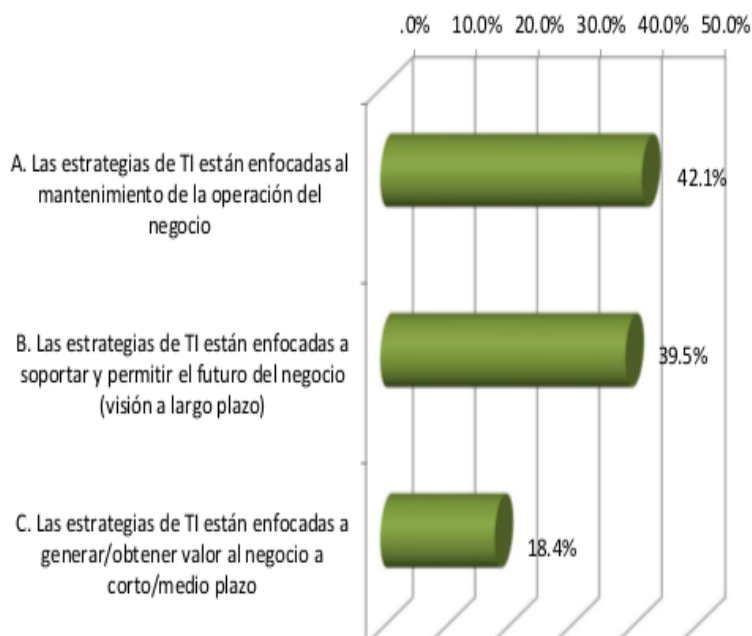


Para el 58,6% TI es muy eficaz a la hora de solucionar problemas de información. El 37,9% considera que TI es medianamente eficaz y el restante 3,5% expresa que TI es totalmente ineficaz a la hora de resolver problemas relacionados con la información.

2.19 Afirmaciones aplicables a la organización

¿Cuál de estas afirmaciones es más aplicable a su organización?

Gráfica 27. Afirmaciones aplicables a la organización



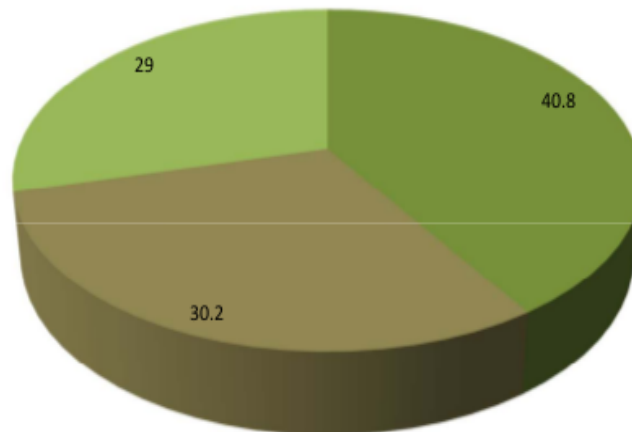
El 42,1% de los entrevistados encuentra más aplicable a su organización la afirmación A.

Para el 39,5% de las empresas, la afirmación que mas se corresponde a su organización es la B y el restante 18,4% encuentra mas aplicable la opción C.

2.19.1 Afirmaciones aplicables a la organización

¿Cuál de estas afirmaciones es más aplicable a su organización?

Afirmaciones aplicables a la organización agrupadas en categorías



- Las estrategias de TI están enfocadas a soportar y permitir el futuro del negocio (visión a largo plazo) // Las estrategias de TI están enfocadas al mantenimiento de la operación del negocio
- Las estrategias de TI están enfocadas a generar/obtener valor al negocio a corto/medio plazo // Las estrategias de TI están enfocadas al mantenimiento de la operación del negocio
- Las estrategias de TI están enfocadas a soportar y permitir el futuro del negocio (visión a largo plazo) // Las estrategias de TI están enfocadas a generar/obtener valor al negocio a corto/medio plazo

2.2 Grado de alineamiento entre la estrategia o visión global de TI y la estrategia o visión global de la organización

¿Cómo describiría el grado de alineamiento entre la estrategia o visión global de TI y la estrategia o visión global de la organización?

Grado de alineamiento	% de casos
Bueno	60,0%
Medio	16,7%
Bajo	13,3%
Excelente	6,7%
Nulo o inexistente	3,3%

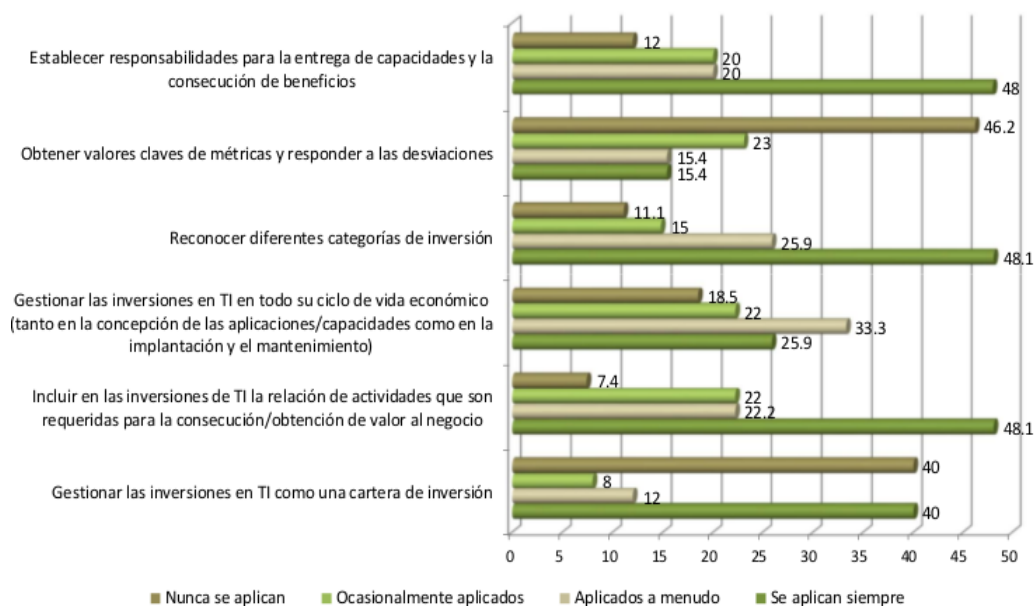
Respecto al grado de alineamiento entre la estrategia de TI y la estrategia de la organización, puede verse, que el 60% de las empresas consultadas lo evalúa como bueno. El 16,7% considera que el grado de alineamiento es medio y para el 13,3% es bajo. Para el 6,7% es excelente el alineamiento entre la estrategia de TI y la de la organización y el 3,3% restante entiende que es nulo o inexistente.

3. APORTACIÓN DE VALOR

3.1 Principios asociados a las inversiones de TI

¿Cuáles de los siguientes principios asociados a las inversiones en TI se están aplicando, o se piensan aplicar, en su organización?

Gráfica 28. Principios asociados a las inversiones de TI

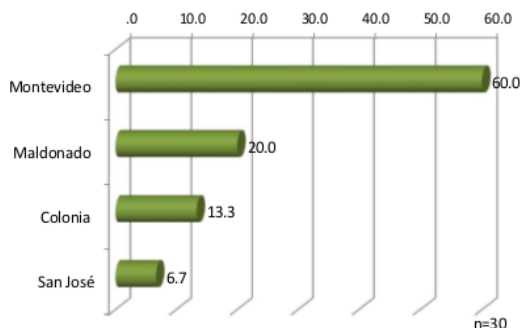


3.2 Dimensión y estructura de la empresa

Rubro y departamento donde se ubica la empresa.

Rubro de la empresa	% de casos
Servicio de TI	16,7
Educación en gastronomía	16,7
Servicio de mecánica automotriz	6,7
Esterilizaciones de materiales médicos	6,7
Andamio y estructura	3,3
Medicina deportiva	3,3
Servicio de telefonía celular	3,3
Fabricación e importación de productos de limpieza.	3,3
Procesamiento de cuero para la industria automotriz	3,3
Hotelería	3,3
Mayorista en computación	3,3
Análisis clínico	3,3
Seguridad	3,3
Productos lácteos	3,3
Vitivinicultura	3,3
Diseño gráfico-publicidad	3,3
Fábrica de gases	3,3
Alimentación balanceada para nutrición animal	3,3
Bazar	3,3
Consultoría en costos y eficiencia energética	3,3

Gráfica 1. Departamento donde se ubica la empresa



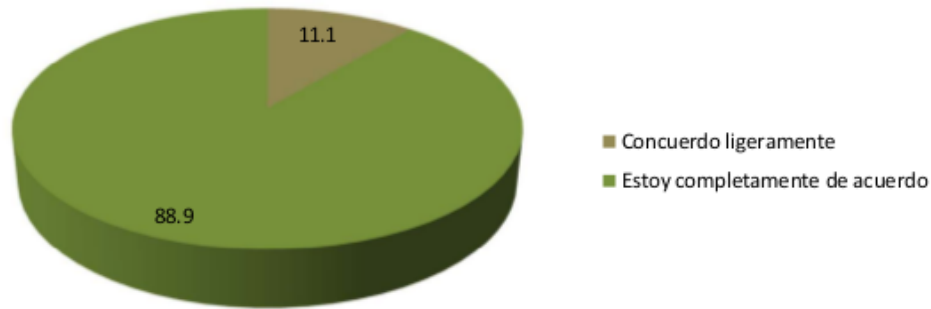
El 16.7% de las empresas pertenecen al rubro servicio de TI y a educación en gastronomía. El 6,7% se encuentra en el rubro de servicio de mecánica automotriz y esterilizaciones de materiales médicos.

Respecto a el departamento donde se ubican las empresas, más de la mitad se encuentra en Montevideo.

3.3 Aporte de las inversiones en TI al valor de la organización

Las inversiones en TI han aportado valor a su organización. ¿De qué forma concuerda con esta afirmación?

Gráfica 30. Aporte de las inversiones

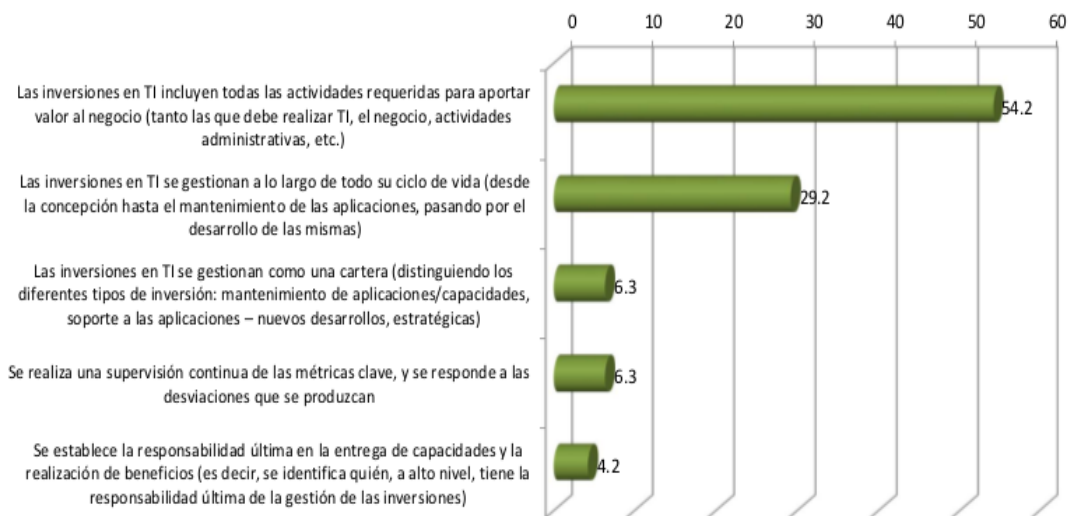


El 88,9% de las empresas consultadas, esta completamente de acuerdo con que las inversiones en TI han aportado valor a su organización. El restante 11,1% concuerda ligeramente con la anterior afirmación.

3.4 Prácticas que aportan mayor valor a las inversiones en TI

¿Cuál de las siguientes prácticas aportan, en su opinión, mayor valor a las inversiones en TI?

Gráfica 31. Prácticas que aportan mayor valor a las inversiones en TI



El 55% de los entrevistados entendieron que la práctica que más aporta valor a las inversiones en TI tiene que ver con que las inversiones incluyen todas las actividades requeridas para aportar valor al negocio. Según el 30% las prácticas que más aportan refieren a que las inversiones se gestionan a lo largo de todo un ciclo de vida, que comienza desde la concepción, el mantenimiento de las aplicaciones pasando por el desarrollo de las mismas.

3.5 y 3.6 Medición del aporte de TI al negocio

Su organización, ¿mide la aportación de las TI al negocio? En caso afirmativo, indique cómo lo hace

Gráfica 32. Medición del aporte de TI al negocio

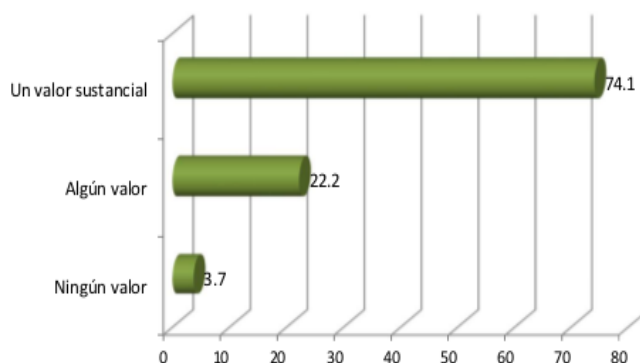


El 60% de las empresas mide la aportación de TI al negocio y el 40% se caracteriza por no medirlo. De las empresas que miden la aportación de las TI, el 60% lo hace a través de matrices e indicadores de calidad. El 30% expresa que lo mide por indicadores como: performance, tiempos promedios, etc. Y el 10% restante lo hace por la medición en las la tasas de error en los procesos.

3.7 Valor obtenido de TI

¿Qué valor cree que su organización está obteniendo de la TI? (Por ejemplo, asociado a mejores relaciones con clientes, mejor gestión del riesgo, costos más bajos, mayor productividad, mayor liderazgo de producto, etc.)

Gráfica 33. Valor obtenido de TI



El 74,1% de las empresas cree que TI le da un valor sustancial a su organización. Para el 22,2% de los entrevistados su organización obtiene algún valor de la TI, y el restante 3,7% cree que no obtiene ningún valor de TI.

3.8 Métricas o indicadores más importantes para confirmar el éxito de las TI en su organización

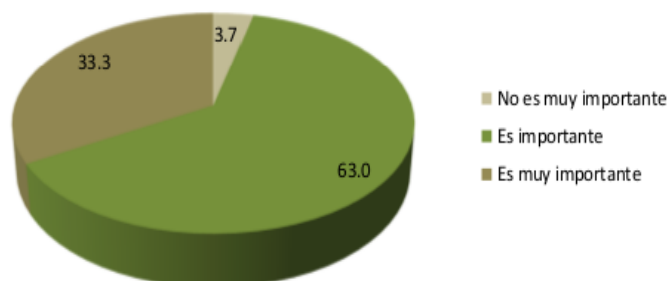
¿Puede indicar tres métricas o indicadores más importantes que utiliza para confirmar el éxito de las TI en su organización?

Métricas o indicadores	% de casos
Sistema de gestión: cantidad de caídas en el mes, cantidad de accesos en el mes, tiempos de acceso.	19,4%
Porcentaje de cumplimiento de proyectos	12,9%
Se evalúa el estado del comportamiento de determinada variable y la desviación de la misma en cuanto a elementos intrínsecos y del ambiente	9,7%
Porcentaje de defecto de sistemas	9,7%
Porcentaje de desviaciones e incidentes y solución de problemas	9,7%
% de la calidad del servicio de TI	9,7%
Porcentaje de aprendizaje de los usuarios (a través de encuestas)	6,5%
Satisfacción del cliente	6,5%
Resultados en áreas asistenciales y económico financieras	3,2%
Se realiza una comparación histórica	3,2%
Reducción de stock cooperativo	3,2%
Sitio web: cantidad mensual de accesos por país.	3,2%
Sistema de telefonía: cantidad de llamadas/servicios utilizados por destino, por duración, etc.	3,2%

3.9 Importancia de la gestión de riesgo en su organización

¿Qué importancia tiene la gestión de riesgos en su organización?

Gráfica 34. Importancia de la gestión de riesgo

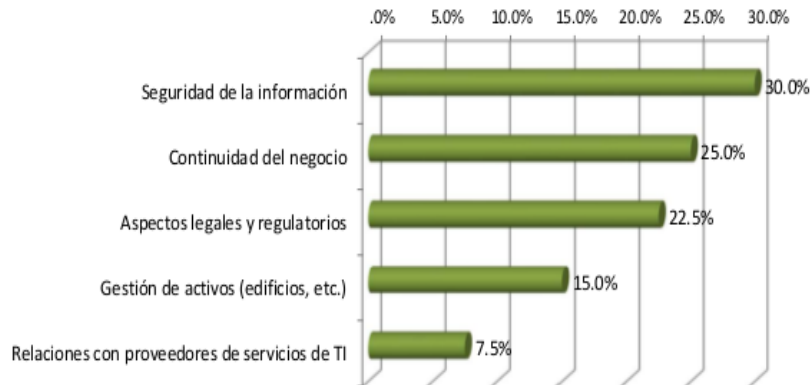


Para el 63% de las empresas consultadas, es importante la gestión de riesgo en su organización. El 33,3% considera que es muy importante la gestión de riesgo y el 3,7% expresa que no es muy importante esta gestión en su organización.

3.10 Áreas en que se realiza la gestión de riesgo

Indique, si se realiza una gestión de riesgos, y en qué áreas o aspectos se realiza

Gráfica 35. Áreas en que se realiza la gestión de riesgo



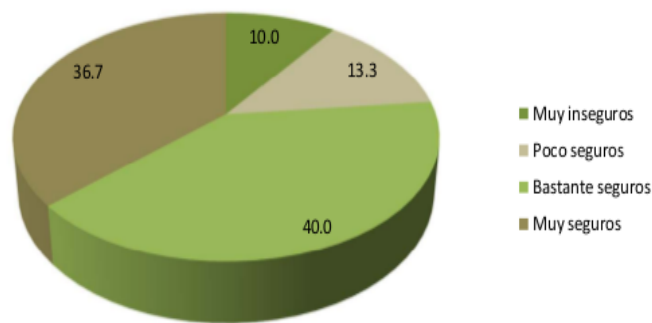
El 30% de las empresas consultadas realiza una gestión de riesgo en el área de seguridad de la información. El 25% explica que realiza esta gestión en aspectos de continuidad del negocio y cuestiones legales-regulatorias. Según el 15% la gestión de activos es una de las áreas donde se realiza la gestión de riesgo y para el restante 7,5% de los entrevistados la gestión se aplica a las relaciones con proveedores de servicio de TI.

4. SEGURIDAD

4.1 Valoración de la seguridad en general de los servicios de TI de su empresa

¿Cómo estima la seguridad en general de los servicios de TI de su empresa?

Gráfica 36. Valoración de la seguridad

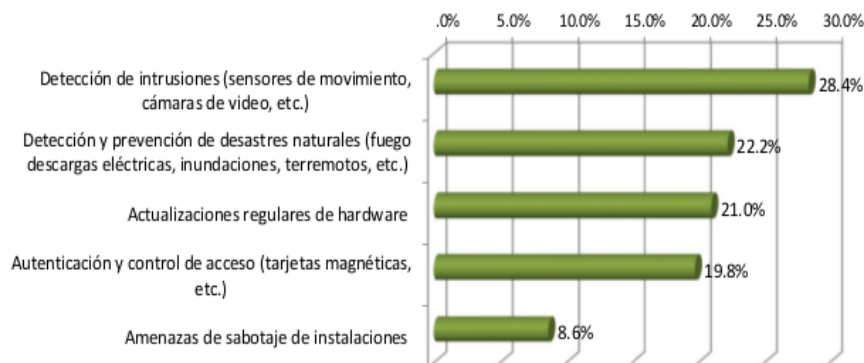


Para el 40% de los entrevistados, los servicios de TI son bastante seguros. Según el 36,7% lo considera como muy seguro y el 13,3% entiende que son poco seguro. El 10% restante evalúa como muy inseguro a los servicios TI de su empresa.

4.2 Tipo de seguridad física aplicable respecto a TI

¿Qué tipo de seguridad física aplica con respecto a TI?

Gráfica 37. Tipo de seguridad física aplicada

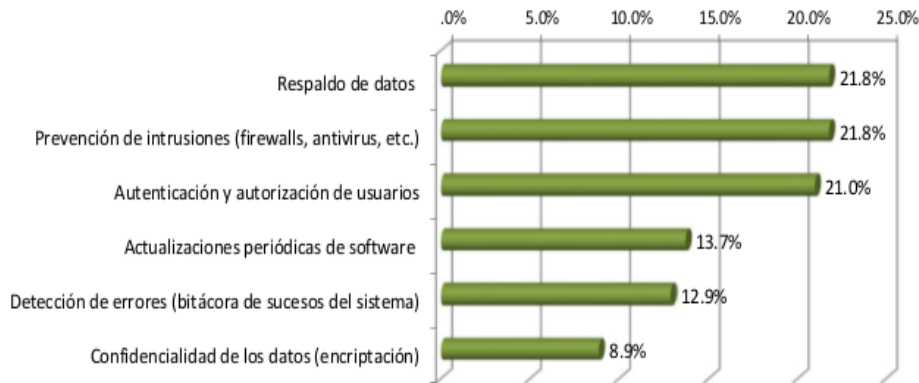


El 28,4% de las empresas aplica como medida de seguridad física la detección de intrusiones. El 22,2% utiliza la detección y prevención de desastres naturales. Según el 21% de los entrevistados, la actualización regular de hardware es la medida que se aplica con respecto a TI. También la autenticación y control de acceso es un tipo de seguridad física que se aplica en el 19,8% de las empresas.

4.3 Tipo de seguridad lógica aplicable respecto a la información de TI

¿Qué tipo de seguridad lógica aplica con respecto a la información de TI?

Gráfica 38. Tipo de seguridad lógica aplicada

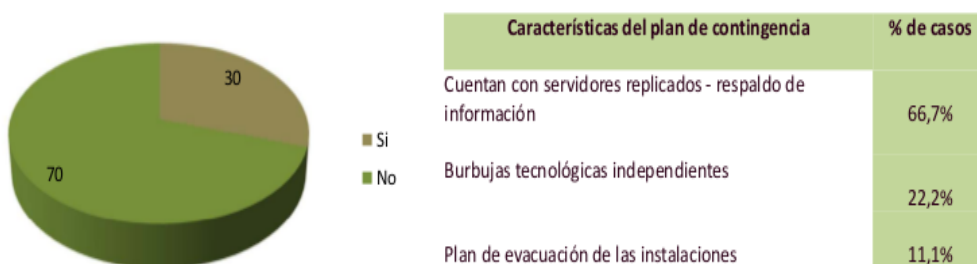


El tipo de seguridad lógica que más se aplica con respecto a la información de TI tiene que ver con el respaldo de datos y con la prevención de intrusiones. Para el 21% de las empresas consultadas, la medida utilizada refiere a la autenticación y autorización de usuarios.

4.4 Plan de recuperación de desastres

¿Cuenta con un plan de recuperación de desastres? En caso afirmativo explicita brevemente.

Gráfica 39. Cuenta con plan de recuperación de desastre

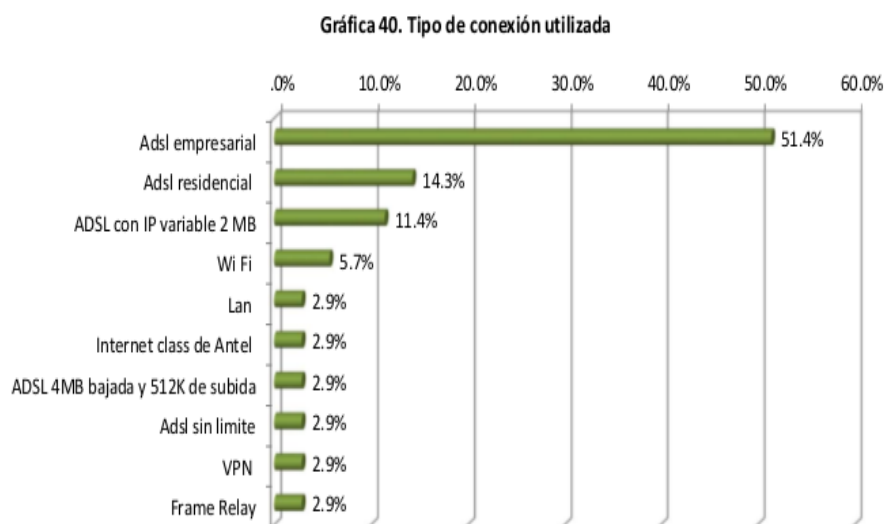


El 70% de las empresas no cuenta con un plan de recuperación de desastre. El restante 30% se caracteriza por si poseer un plan de contingencia. De las empresas que poseen dicho plan, el 66,7% se caracteriza por ser un plan en donde se cuenta con servidores replicados. Para el 22,2% de los entrevistados, el plan se define como burbujas tecnológicas independientes y según el 11,1% lo define como un plan de evacuación de las instalaciones.

5. INTERNET

5.1 y 5.2 Acceso a internet y tipo de conexión que utiliza

¿Tiene acceso a Internet? En caso afirmativo, ¿qué tipo de conexión utilizan?



El 100% de las empresas tiene acceso a internet.
 El tipo de conexión que más se utiliza es el ADSL empresarial con un 51,4%.
 El 14,3% usa el ADSL residencial para conectarse a internet y el 11,4% lo hace a través de ADSL con IP variable 2 MB.

5.3 Fines para que utiliza internet

¿Con que fines se utiliza Internet?

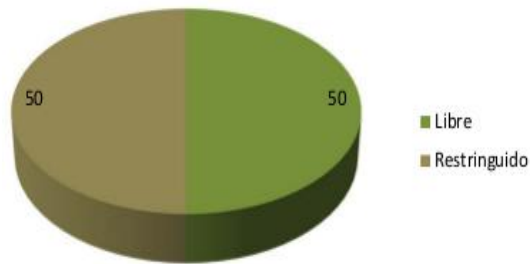
Fines de utilización	% de casos
Información y mail	54,9%
Acceso de clientes	23,5%
Proveedores al software de gestión	7,9%
Aplicación de SAS	7,9%
Operaciones bancarias	3,9%
Esparcimiento	2,0%
Cursos online	2,0%
Comunicación con funcionarios de otras empresas	2,0%

Casi el 55% de los entrevistados expresa que utiliza internet para informarse y consultar mails.
 Para el 23,5% el fin de utilización es para el acceso de clientes.
 El 7,9% usa internet para la aplicación de SAS y también un 7,9% lo utiliza como proveedores al software de gestión.

5.4 Tipo de acceso de usuarios a internet

¿Cómo es el acceso de los usuarios a Internet?

Gráfica 41. Tipo de acceso de usuario

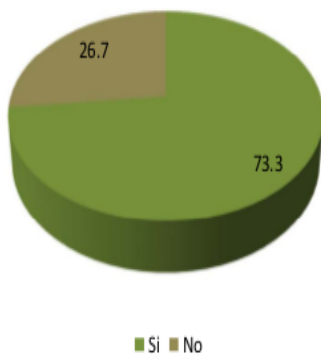


El 50% de las empresas tiene un acceso libre de los usuarios a internet. El otro 50% se caracteriza por restringir el acceso de los usuarios.

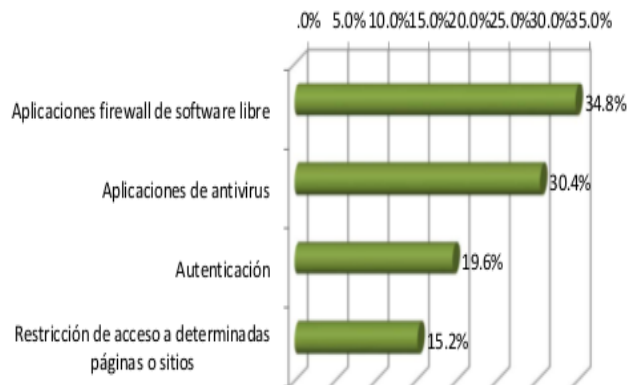
5.5 y 5.6 Mecanismos de seguridad para el acceso a internet

¿Cuenta con mecanismos de seguridad para el acceso a Internet? ¿Cuáles son esos mecanismos?

Gráfica 42. Cuenta con mecanismo de seguridad



Gráfica 43. Tipo de mecanismo de seguridad

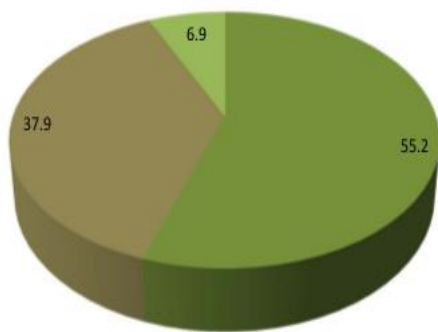


El 73% de las empresas consultadas cuenta con mecanismos de seguridad para el acceso a internet. De las empresas que cuentan con estos mecanismos, el 34,8% se caracteriza por aplicar firewall como mecanismo. El 30% aplica antivirus y el 20% usa la autenticación como forma de seguridad en el acceso a internet.

5.7 Importancia de contar con un sitio web institucional

¿Cree que es importante el contar con un sitio web institucional?

Gráfica 44. Importancia de sitio web



■ Muy importante ■ Importante ■ Nada importante

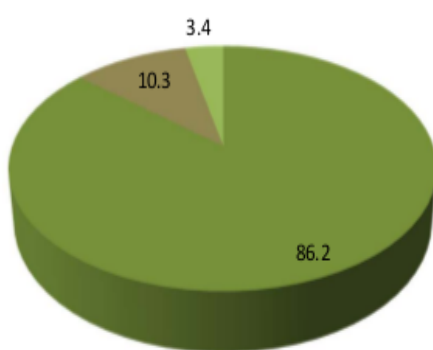
El 55% de los entrevistados, entiende que es muy importante contar con un sitio web institucional.

Según el 37%, es importante el sitio web y el restante 6,9% evalúa como nada importante contar con un sitio web.

5.8 y 5.9 Cuenta con un sitio web y como es

¿Cuenta con un sitio Web institucional? Si tiene sitio web institucional ¿cómo es el sitio?

Gráfica 45. Cuenta con un sitio web institucional



■ Sí ■ No ■ En construcción

Como es el sitio	% de casos
Dinámico	53,1%
Estático	28,1%
Interactivo	9,4%
Portal	6,3%
Carrito de compras	3,1%

El 86,2% de las empresas cuenta con un sitio web institucional. El 10,3% no cuenta con el mismo y el 3,4% de los entrevistados expresa que el sitio está en construcción.

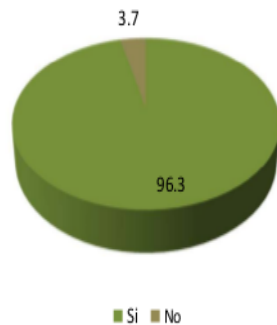
De aquellas empresas que cuenta con un sitio web, el 53,1% se caracteriza por ser dinámico y el 28,1% por ser estático.

5.10 Importancia del sitio web para apoyar y favorecer los objetivos estratégicos de la organización

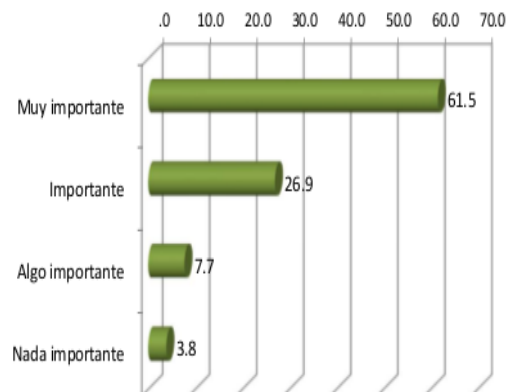
¿Cree Ud. que el sitio web institucional apoya y favorece los objetivos estratégicos de la organización?

Si la respuesta es afirmativa ¿De qué manera?

Gráfica 46. Sitio web como apoyo a los objetivos de la organización



Gráfica 47. Importancia del sitio web como apoyo



El 96,3% de los entrevistados, considera que el sitio web institucional apoya y favorece los objetivos estratégicos de la organización. Para el 61,5% es muy importante el apoyo a los objetivos de la organización. El 26,9% considera que es importante y el 7,7% evalúa como algo importante el sitio web como apoyo a la estrategia de la organización.

5.11 Utilidad, beneficio y valor que aporta el sitio web

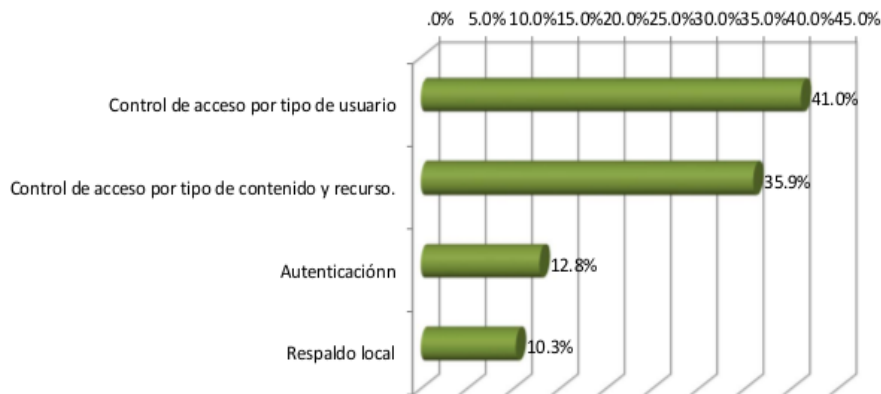
¿Qué utilidad, beneficios y valor le aporta el sitio web?

Utilidad que aporta el sitio web	% de casos
Acceso a información genérica de la empresa por parte de potenciales clientes	40,5%
Presencia en el mercado	37,8%
información general	5,4%
Facilidad operativa	5,4%
Mejora la gestión de datos	5,4%
Interacción con los alumnos	2,7%
Clientes pueden ver información de la mercadería entregada	2,7%

5.12 Políticas y procesos de seguridad para proteger los datos

¿Utiliza políticas y procesos de seguridad para proteger los datos? ¿Si lo hace, que políticas, procesos y prácticas utiliza para controlar el acceso a la información?

Gráfica 48. Políticas utilizadas para controlar el acceso a la información

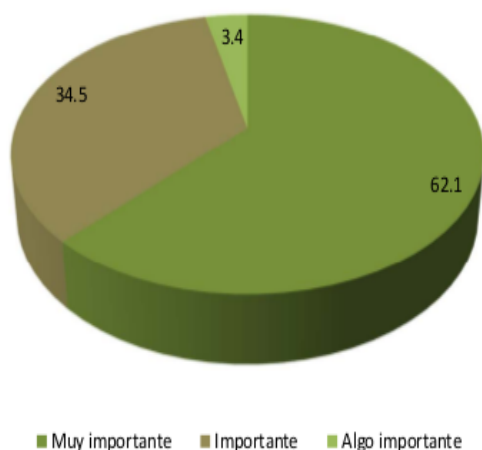


El 100% de las empresas consultadas cuenta con políticas de seguridad para proteger los datos.
 El 41% utiliza el control de acceso por tipo de usuario como política de seguridad.
 Quienes utilizan el control de acceso por tipo de contenido y recurso son el 35,9% de los entrevistados.
 El 12,8% usa la autenticación y el restante 10,3% utiliza el respaldo local como proceso de seguridad.

5.13 Importancia de la seguridad de la información en la organización

¿Qué nivel de importancia tiene para Ud. la seguridad de la información en la organización?

Gráfica 49. Importancia de la seguridad de la información



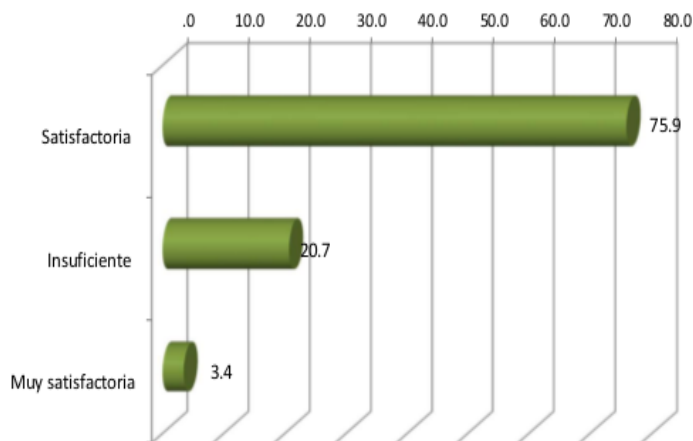
Según el 62% es muy importante la seguridad de la información en la organización.

El 34% lo evalúa como importante la seguridad y el 3,4% entiende que es algo importante.

5.14 Evaluación de las políticas de seguridad en su organización

¿Cómo considera que son las políticas, prácticas y procesos de seguridad de la información en su organización?

Gráfica 50. Evaluación de las políticas de seguridad

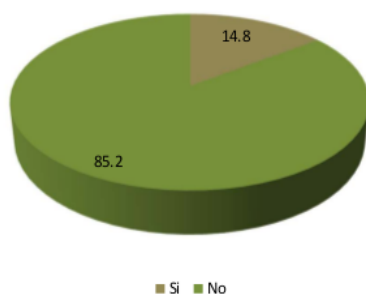


En el total, 3 de cada 4 entrevistados, evalúa como satisfactoria las prácticas de seguridad de la información en la organización. El 20,7% entiende que son insuficientes las políticas de seguridad y el 3,4% considera que son muy satisfactorias estos procesos de seguridad de la información.

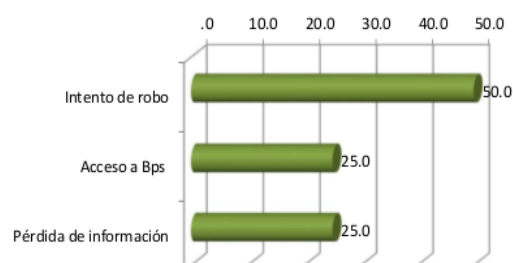
5.15 Problema en relación a un acceso indebido a la información

¿Ha sufrido algún problema en relación a un acceso indebido a la información? ¿Qué tipo de problema ha tenido?

Gráfica 51. ¿ Ha tenido problema en relación a acceso indebido a la información?



Gráfica 52.Tipo de problema

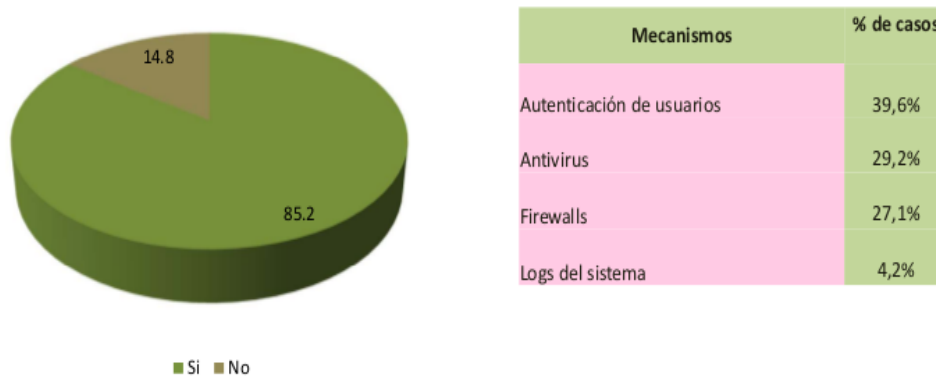


El 85% de las empresas consultadas expresa que no ha tenido problemas en relación a acceso indebido a la información. El 14,8% manifiesta que si ha tenido este tipo de problemas. De las empresas que han tenido problema, el 50% tienen que ver con intento de robo, el 25% refiere a problemas en el acceso a BPS y el restante 25% refiere a pérdida de información.

5.16 Mecanismos de protección contra acceso indebido a la información

¿Existen mecanismos de protección contra accesos indebidos a la información? Si existen ¿Cuáles son estos mecanismos?

Gráfica 53. ¿ Existen mecanismos de protección contra acceso indebido a la información

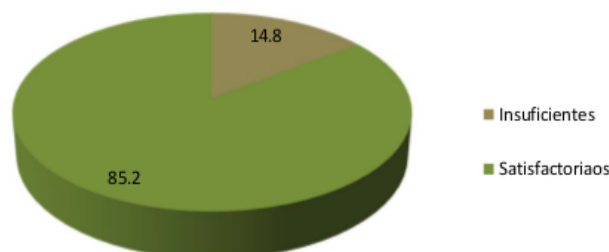


El 15% de las empresas cuenta con mecanismos de protección contra acceso indebido a la información. En estas empresas, el mecanismo de protección más frecuente con un 40%, tiene que ver con la autenticación de usuarios. El 30% utiliza el antivirus como forma de proteger accesos indebidos y el 27% se caracteriza por usar firewall. Finalmente el 4,2% usa logs del sistema para proteger el acceso.

5.17 Evaluación de los mecanismos de protección contra los accesos indebidos a la información

¿Cómo considera que son los mecanismos de protección contra los accesos indebidos a la información?

Gráfica 54. Evaluación de los mecanismos de protección



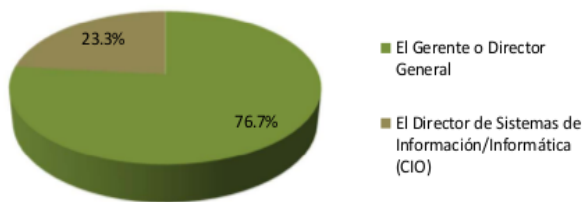
Para el 85% los mecanismos de protección contra los accesos indebidos son satisfactorios. El 15% evalúa como insuficientes estos tipos de mecanismos de protección.

6. TOMA DE DECISIONES

6.1 Líder de la gobernanza de TI en la organización

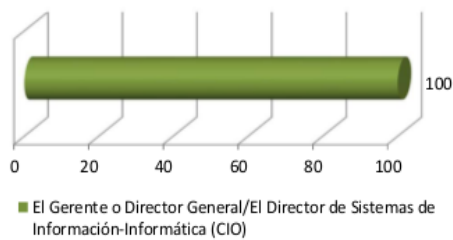
¿Quién considera que es el líder de la gobernanza de TI en la organización?

Gráfica 55. Líder de TI en la organización



En el 76% de las empresas, quien lidera la gobernanza de TI en la organización es el gerente o director general. El restante 23% expresa que quien lidera la gobernanza es el director de sistemas de Información/informática.

Categorías agrupadas de Líder de TI en la organización

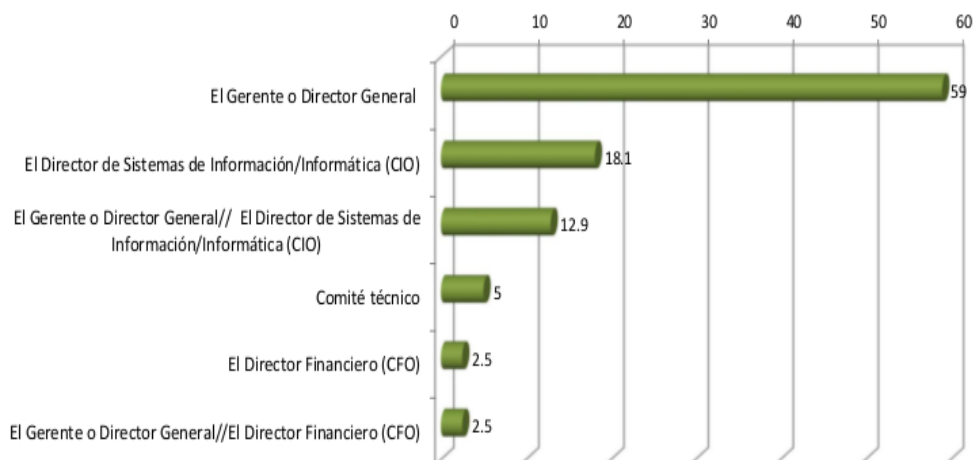


Si analizamos quien es el líder de la gobernanza de TI en categorías puede verse que el 100% de las empresas especifica que quien lidera la gobernanza es el gerente general conjuntamente con el director de sistema de información-informática.

6.1.1 Líder de la gobernanza de TI en la organización

¿Quién considera que es el líder de la gobernanza de TI en la organización?

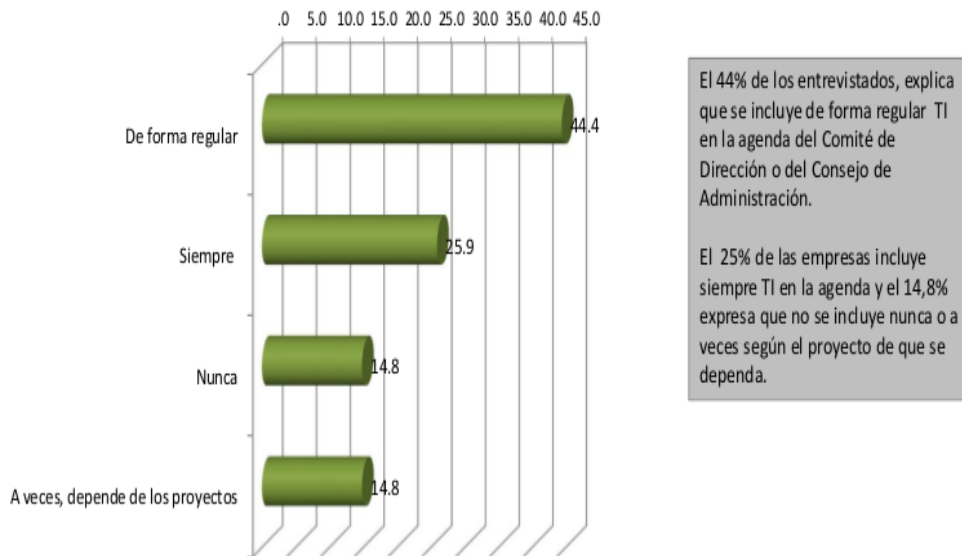
Gráfica 55. Líder de TI en la organización



En el 59% de las empresas, quien lidera la gobernanza de TI en la organización es el gerente o director general. El restante 18,1% expresa que quien lidera la gobernanza es el director de sistemas de Información/informática.

6.2 Frecuencia de incluir TI en la agenda del Comité de Dirección o del Consejo de Administración

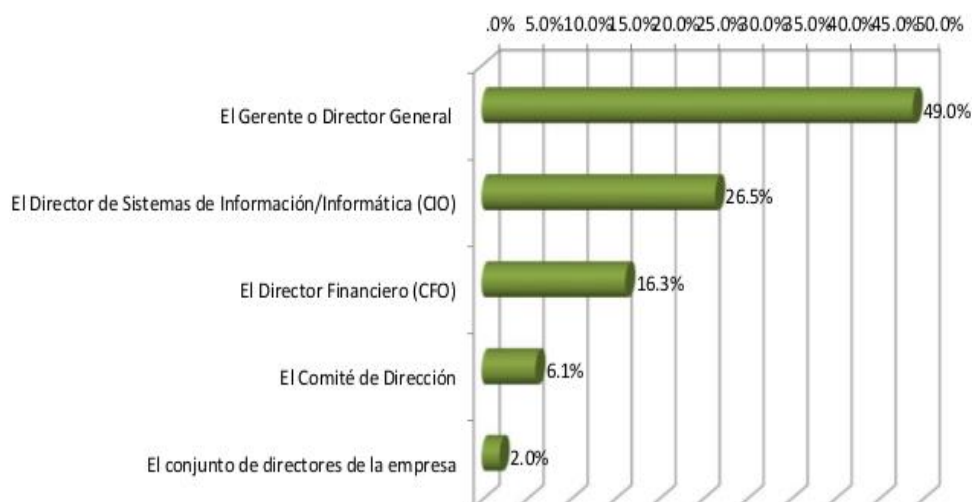
¿Con qué frecuencia se incluyen la TI en la agenda del Comité de Dirección o del Consejo de Administración?



6.3 Toma de decisiones sobre TI en la organización

¿Quién toma las decisiones sobre TI en su organización?

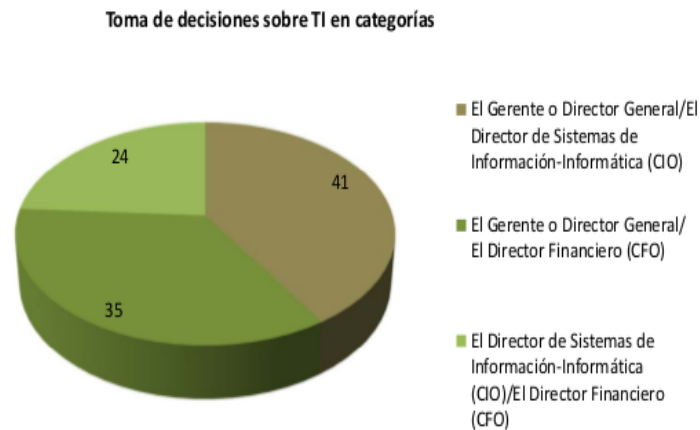
Gráfica 57. Toma de decisiones sobre TI



En el 49% de las empresas quien toma las decisiones sobre TI es el gerente o director general. El 26% de los entrevistados, explica que es el director de sistemas de información quien toma las decisiones. Y para el 16,3% de las empresas quien toma las decisiones es el director financiero.

6.3 .1 Toma de decisiones sobre TI en la organización

¿Quién toma las decisiones sobre TI en su organización?

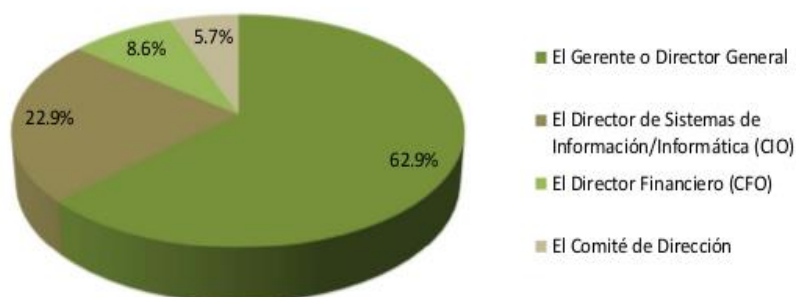


Si se analiza quien toma las decisiones sobre TI en la organización, puede verse que el 41% expresa que lo hace el gerente general y el director de sistemas de información-informática. El 35% explica que quien toma las decisiones son el gerente general con el director financiero y según el 24% quien se encarga de esta actividad es el director de sistemas de información-informática en conjunto con el director financiero.

6.4 Seguimientos de las decisiones tomadas sobre TI

¿Quién realiza el seguimiento de las decisiones tomadas sobre TI en su organización?

Gráfica 58. ¿Quién realiza el seguimiento de las decisiones tomadas sobre TI?

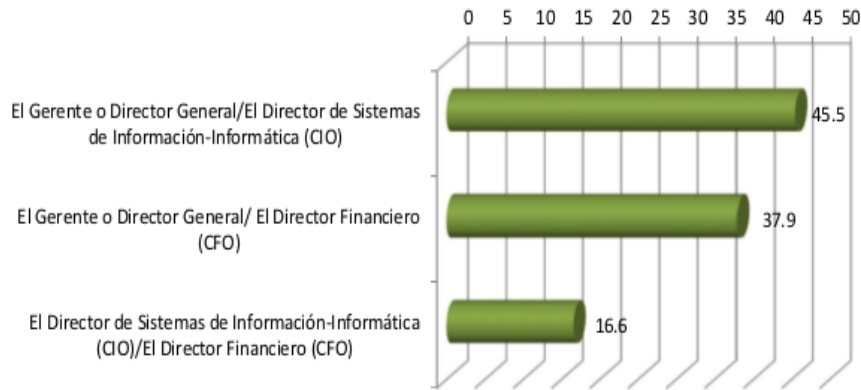


En el 62,9% de las empresas quien realiza el seguimiento de las decisiones tomadas sobre TI es el gerente o director general. El 22% explica que es el director de sistema de Información quien realiza el seguimiento y para el 8,6% de los casos entrevistados, es el director financiero quien se encarga de realizar esta actividad.

6.4 .1 Seguimiento de las decisiones tomadas sobre TI

¿Quién realiza el seguimiento de las decisiones tomadas sobre TI en su organización?

Seguimiento de las decisiones sobre TI en categorías

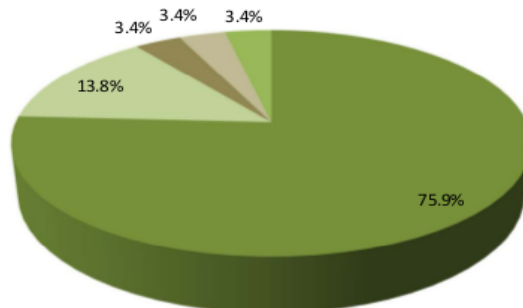


Si se analiza quien realiza el seguimiento de las decisiones tomadas sobre TI en la organización, puede verse que el 45% expresa que hace el gerente general y el director de sistemas de información-informática. El 37% explica que quien toma las decisiones son el gerente general con el director financiero y según el 16% quien se encarga de esta actividad es el director de sistemas de información-informática en conjunto con el director financiero.

6.5 Responsable último de la ejecución de las decisiones tomadas sobre TI

¿Quién es el responsable último de la ejecución de las decisiones tomadas sobre TI en su organización?

Gráfica 59. Responsable último de la ejecución de las decisiones de TI

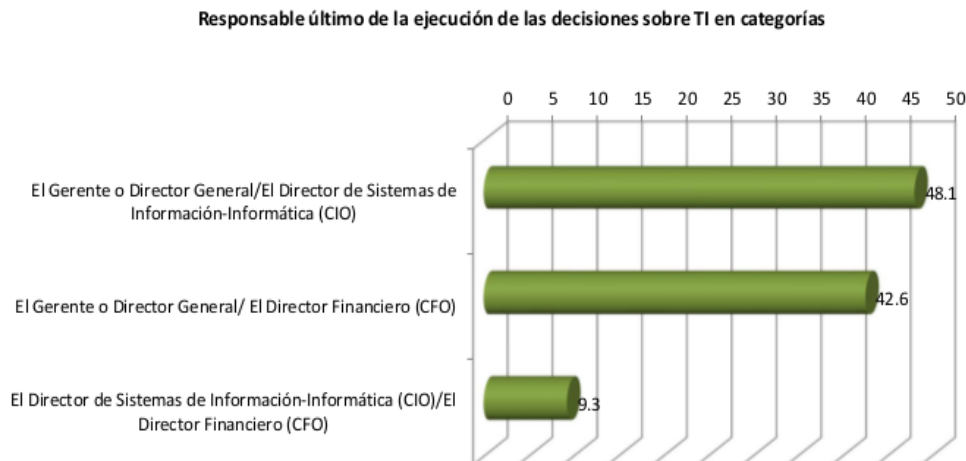


El 97% de las empresas consultadas, explica que quien es el responsable de la ejecución de las decisiones de TI son el gerente general, el director de sistema de información y el director financiero.

- El Gerente o Director General
- El Director de Sistemas de Información/Informática (CIO)
- El Director Financiero (CFO)
- El Comité de Dirección
- Empresa que tiene tercerizado el servicio de TI

6.5.1 Responsable último de la ejecución de las decisiones tomadas sobre TI

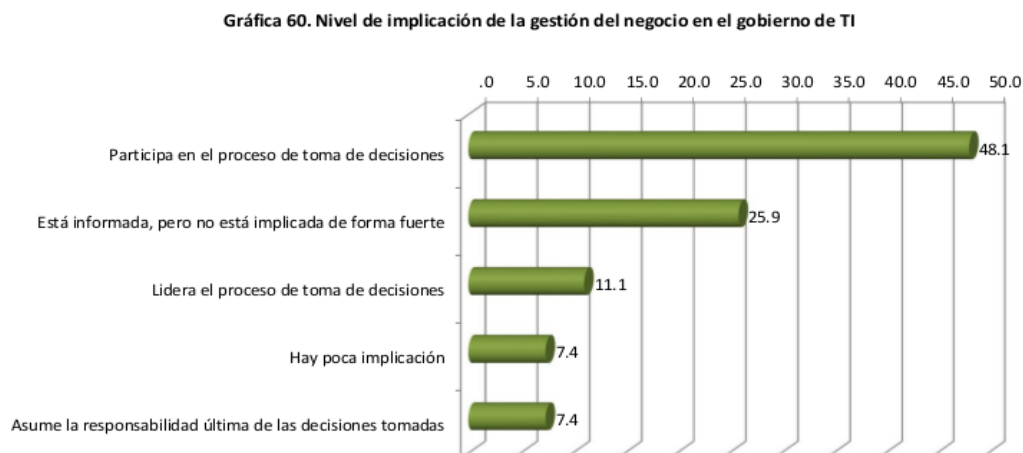
¿Quién es el responsable último de la ejecución de las decisiones tomadas sobre TI en su organización?



Si se analiza quien es el responsable último de la ejecución de las decisiones tomadas sobre TI en la organización, puede verse que el 48% expresa que lo hace el gerente general y el director de sistemas de información-informática. El 42 % explica que quien toma las decisiones son el gerente general con el director financiero y según el 9% quien se encarga de esta actividad es el director de sistemas de información-informática en conjunto con el director financiero.

6.6 Nivel de implicación de la gestión del negocio en el gobierno de las iniciativas de TI asociadas al negocio

¿Cómo describiría el nivel de implicación de la gestión del negocio en el gobierno de las iniciativas de TI asociadas al negocio?



El 48% de las empresas, participa en el proceso de toma de decisiones. El 25% expresa que esta informada, pero no esta implicada de forma fuerte en el gobierno de TI. Y el 11% de los casos, lidera el proceso de toma de decisiones.

6.7 Herramientas usadas para la aprobación de proyectos

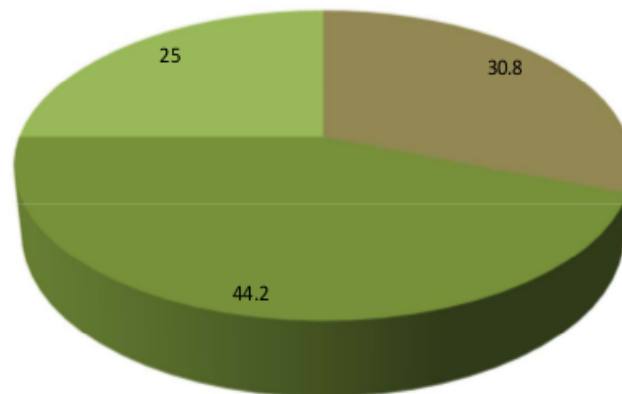
¿Qué herramientas o técnicas se usan para la aprobación de proyectos?

Herramientas para la aprobación de proyecto	% de casos
Se realiza un análisis de viabilidad (business case) con un análisis económico y cualitativo, que incluye la identificación de los riesgos y las alternativas	34,2%
Se realiza un análisis de viabilidad (business case) con un análisis económico (costos y beneficios)	26,3%
Se identifican beneficios tangibles e intangibles, además del costo	21,1%
Se realiza un análisis de viabilidad (business case) con un análisis económico y cualitativo	7,9%
Se realiza un análisis de viabilidad (business case) con un análisis económico (costos) y beneficios Cualitativos	7,9%
Se identifican beneficios tangibles, además del costo	2,6%

6.7.1 Herramientas usadas para la aprobación de proyectos

¿Qué herramientas o técnicas se usan para la aprobación de proyectos?

Herramientas usadas para la aprobación de proyectos en categorías

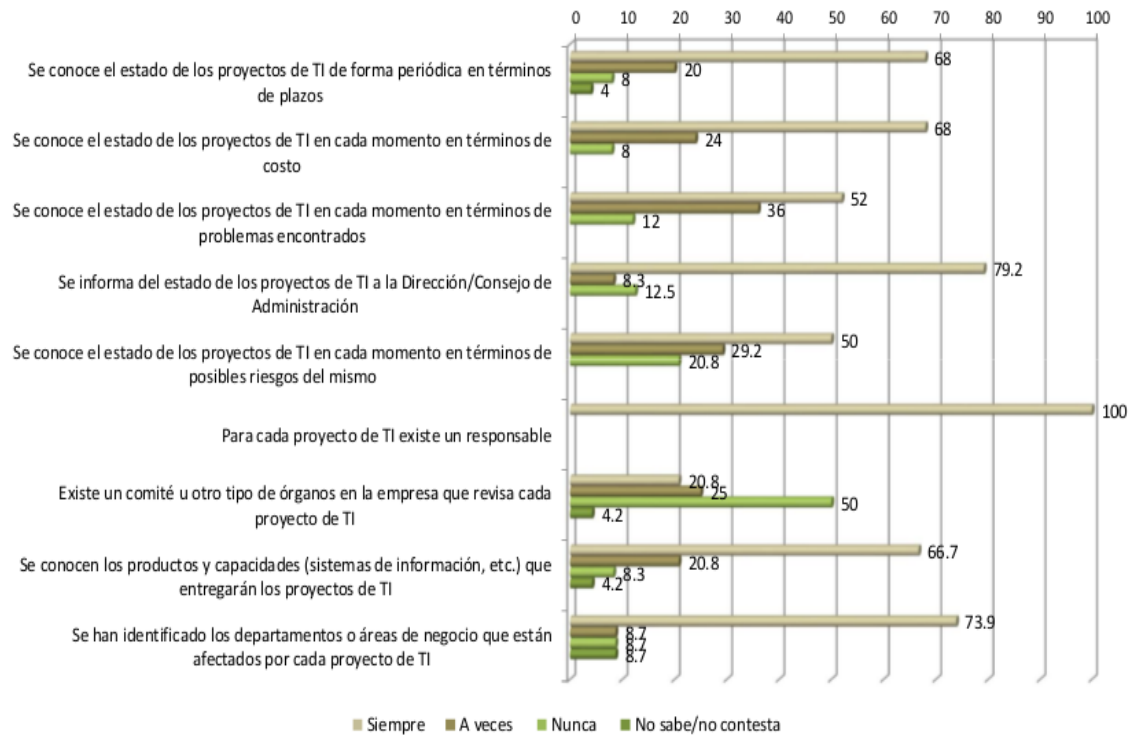


- Se realiza un análisis de viabilidad (business case) con un análisis económico y cualitativo, que incluye la identificación de los riesgos y las alternativas//Se realiza un análisis de viabilidad (business case) con un análisis económico y cualitativo
- Se realiza un análisis de viabilidad (business case) con un análisis económico y cualitativo, que incluye la identificación de los riesgos y las alternativas//Se realiza un análisis de viabilidad (business case) con un análisis económico (costos y benefici
- Se realiza un análisis de viabilidad (business case) con un análisis económico y cualitativo//Se realiza un análisis de viabilidad (business case) con un análisis económico (costos y beneficios)

6.8 Estado de la organización

En lo relativo a los proyectos de TI, indique, para cada afirmación, cuál es el estado en su organización

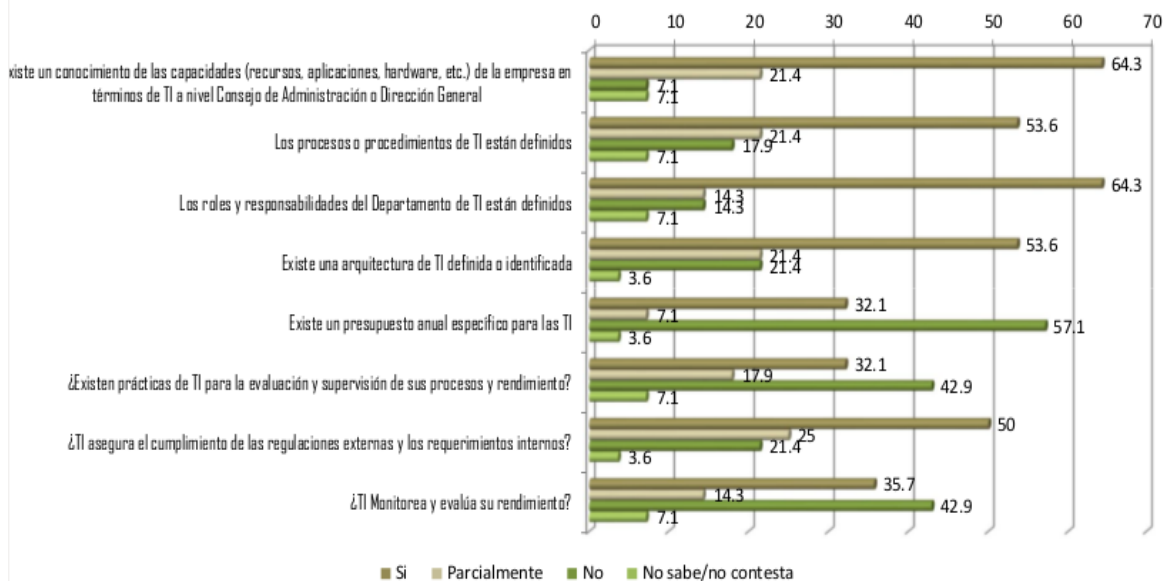
Gráfica 61. Estado de la organización



6.9 Situación de la organización

Indique, para las siguientes afirmaciones, cuál es la situación en su organización

Gráfica 62. Situación de la organización



7. Dimensión y estructura de la empresa

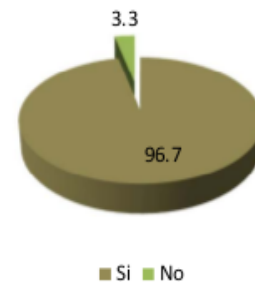
Cantidad de sucursales de la empresa, exportación y mercado interno.

Cantidad de sucursales	
Sucursales	% de casos
0	64,3
1	10,7
2	21,4
3	3,6

Gráfica 2. Exportación



Gráfica 3. Mercado Interno



El 64,3% de las empresas se caracteriza por no tener sucursales. Por su parte el 10,7% tiene una sola sucursal y el 21,4% de las empresas tiene 2. El promedio de sucursales de las empresas es de 0,64 y la mediana es 0.

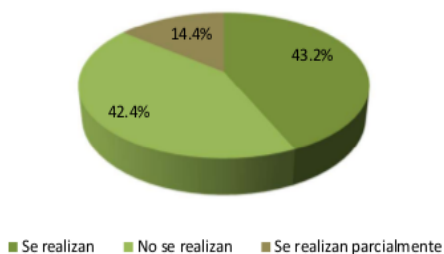
Respecto aquellas empresas que exportan, puede verse que el 72,4% no lo hacen, mientras que el 27,6% si tiene como actividad la exportación.

Esta tendencia también puede verse en la gráfica nº3, donde casi el 100% de las empresas trabaja con el mercado interno.

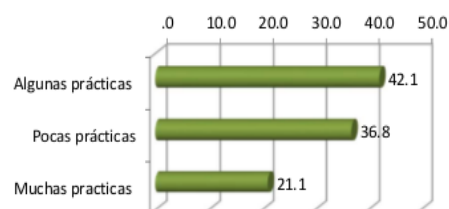
7.1 Realización de prácticas asociadas con el gobierno de las TI

¿Se realizan alguna de las prácticas siguientes asociadas con el Gobierno de las TI en su organización?

Realización de prácticas



Realización de prácticas en intervalos



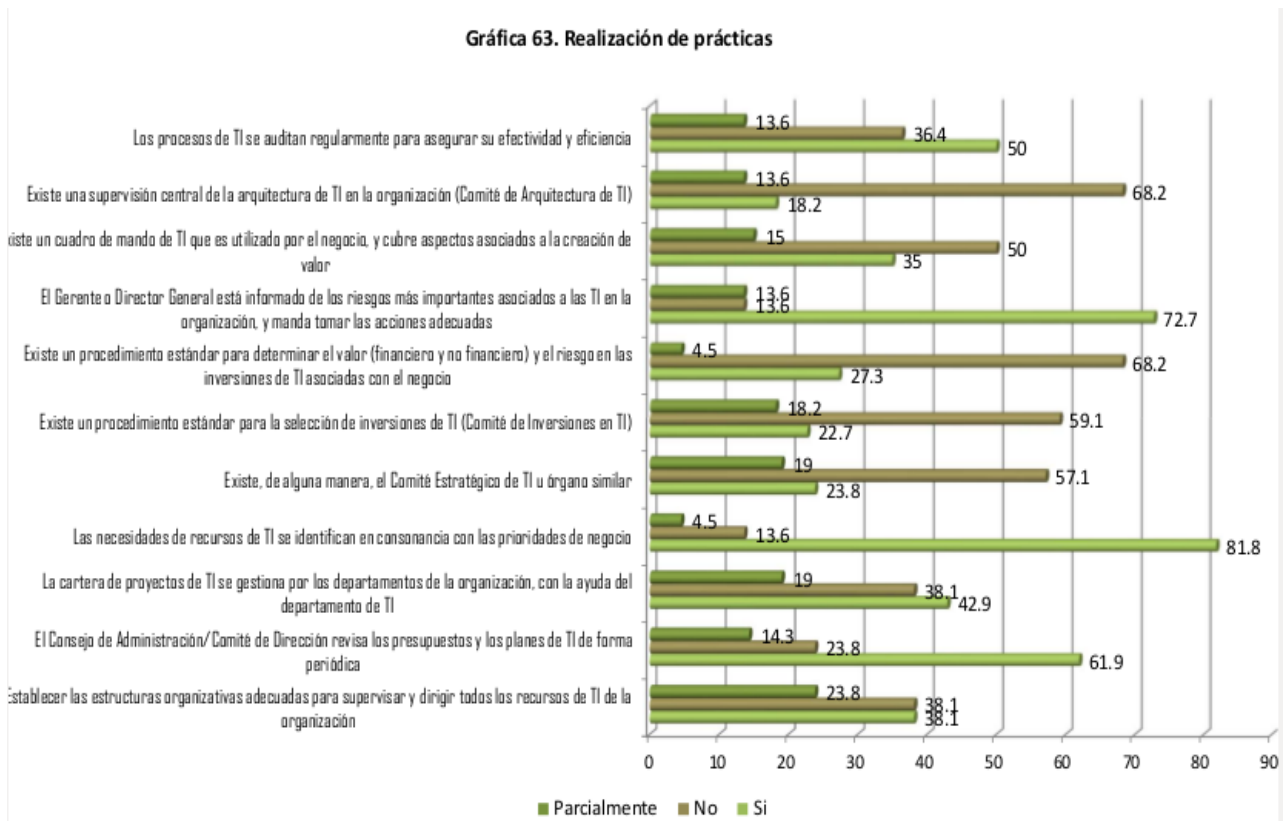
El 43% de las empresas consultadas, realizan prácticas asociadas con el gobierno de TI. El 42% expresa que no realiza estas prácticas y el restante 14% explica que las realiza parcialmente.

En relación a la cantidad de prácticas que se realizan, puede verse que el 42% realiza algunas prácticas y el 36% se caracteriza por efectuar pocas prácticas.

Y el restante 21% expresa que realiza muchas prácticas asociadas con el gobierno de las TI en su organización.

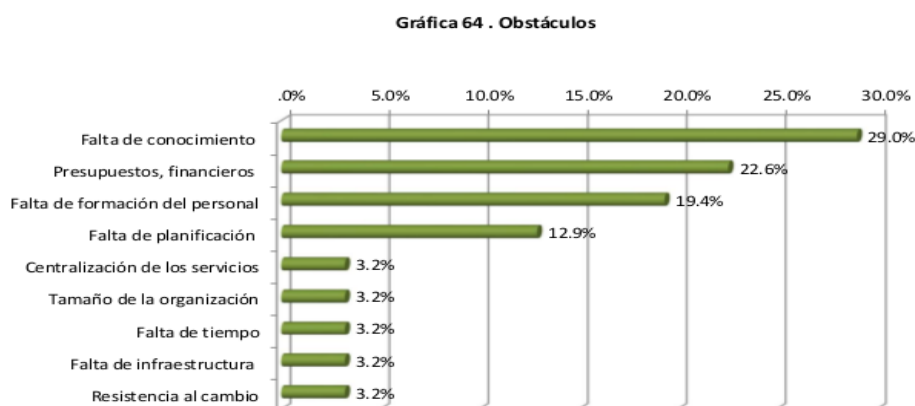
7.1.1 Realización de prácticas asociadas con el gobierno de las TI

¿Se realizan alguna de las prácticas siguientes asociadas con el Gobierno de las TI en su organización?



7.2 Obstáculos para que su organización no adopte las prácticas definidas anteriormente

¿Cuáles son los principales obstáculos o restricciones para que su organización no adopte las prácticas definidas anteriormente?

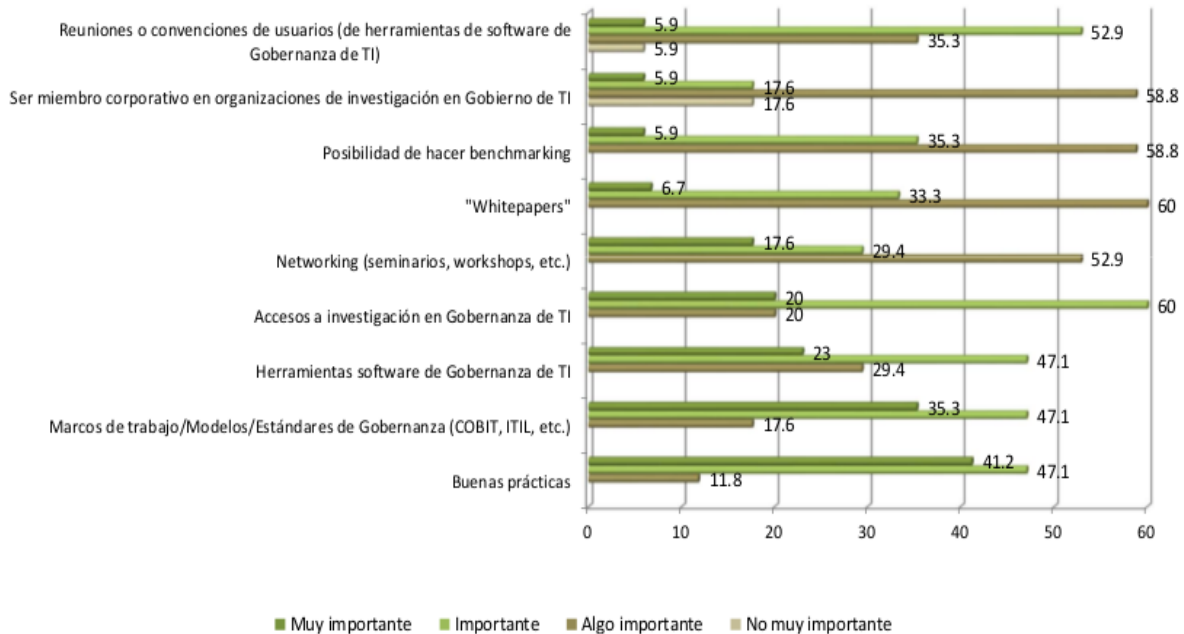


El 29% de las empresas consultadas, entiende que el principal obstáculo para que la organización no adopte las prácticas definidas tiene que ver con la falta de conocimiento. Para el 22% el problema refiere a aspectos económicos y financieros. Y según el 19% la falta de formación del personal constituye un importante obstáculo. También la falta de planificación es un obstáculo para el 12% de los entrevistados.

7.3 Importancia de las siguientes prácticas de gobernanza de TI

¿Qué importancia asignaría a las siguientes prácticas de gobernanza de TI?

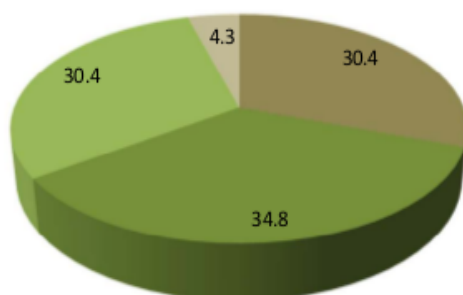
Gráfica 65. Importancia de las siguientes prácticas



7.4 Implementación de prácticas que permitan mejorar la Gobernanza de las TI en su organización

¿Ha implementado, está en proceso, o considera implementar prácticas que permitan mejorar la Gobernanza de las TI en su organización?

Gráfica 66. Implementación de prácticas



- No considero su implementación
- Estoy considerando su implementación
- Estoy en proceso de implementación
- He implementado

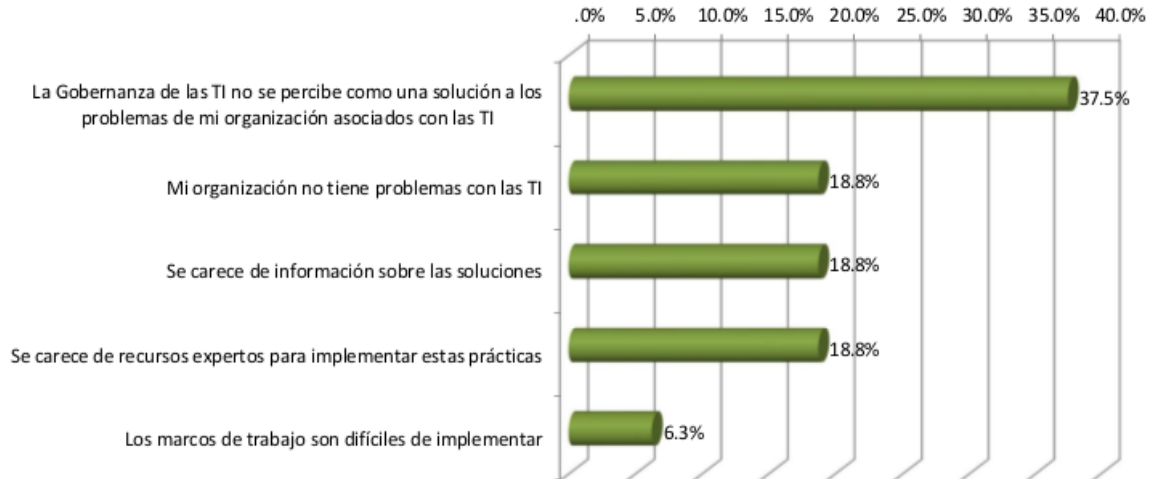
El 34% de las empresas consultadas, expresa que está considerando la implementación de prácticas que permitan mejorar la Gobernanza de las TI en la organización. El 30,4% no considera su implementación.

Por otro lado, quienes ya están en proceso de implementación corresponden a el 30,4% de las empresas y el restante 4,3% menciona que ya ha implementado estas prácticas de mejora.

7.5 Motivo de no implementación de las prácticas

Si no está considerando implementar prácticas en la pregunta anterior, indique el por qué

Gráfica 67. Motivo de no implementación de prácticas



Para el 37% de las empresas consultadas, el principal motivo para no implementar las prácticas tiene que ver con que la gobernanza de las TI no se percibe como una solución a los problemas de la organización. El 18,8% entiende que su organización no tiene problemas con las TI y quienes consideran como problema que se carece de información sobre las soluciones corresponden al 18,8% de los entrevistados. Según el 18,8%, el principal problema refiere a la carencia de recursos expertos para la implementación de esas prácticas.

7.6 Implementación de alguna medida para mejorar en alguno de los siguientes aspectos

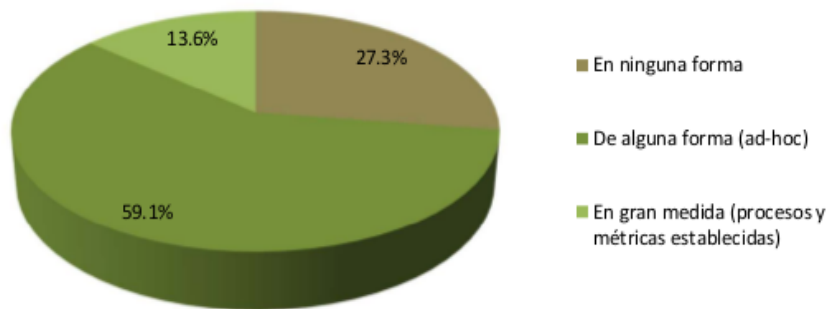
¿Ha implementado o está en proceso de implementar alguna medida para mejorar en alguno de los siguientes aspectos?

Medida	% de casos
Entrega de valor de TI asociada a una mejor relación con los clientes	16,2%
Alineamiento entre la estrategia de TI y la estrategia global del negocio	14,3%
Gestión de recursos de TI (personas, sistemas, datos financieros, etc.)	14,3%
Entrega de valor de TI asociada a una reducción de costos	14,3%
Entrega de valor de TI asociada a un mayor liderazgo/innovación en productos/servicios	12,4%
Gestión activa del ROI (retorno de la inversión) de TI	10,5%
Gestión del riesgo de TI	9,5%
Medidas de rendimiento actual de TI	8,6%

7.7 Medición del progreso en la Gobernanza de TI

En qué grado mide su progreso en la Gobernanza de TI?

Gráfica 68. Medición del progreso en la Gobernanza

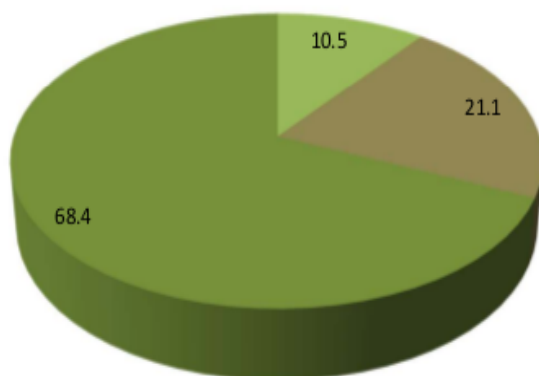


Casi el 60% de los entrevistados, mide de alguna forma (ad-hoc) su progreso en la gobernanza de TI. El 27% explica que no mide su progreso y el restante 13% menciona que mide en gran medida su progreso en la gobernanza de TI.

7.8 Prácticas de Gobernanza de TI como mejora de la eficiencia de los costos de TI para el negocio

¿Cree que las prácticas de Gobernanza de TI han permitido mejorar la eficiencia de los costos de TI para el negocio?

Gráfica 69. Práctica como mejora de eficiencia



El 68% de los entrevistados, entiende que las prácticas de Gobernanza de TI ciertamente mejoran la eficiencia de los costos para el negocio. El 21% cree que sirven para mejorar y el 10% entiende que estas prácticas no mejoran la eficiencia de los costos.

■ No lo creo ■ Lo creo ■ Ciertamente

8. CONOCIMIENTO DE HERRAMIENTAS Y ORGANIZACIONES DE GOBERNANZA DE TI

8.1 Organizaciones que proporcionan o implementan soluciones a problemas de Gobernanza de TI

¿Cuál de las siguientes organizaciones conoce que proporcionan o implementan soluciones a los problemas de Gobernanza de TI?



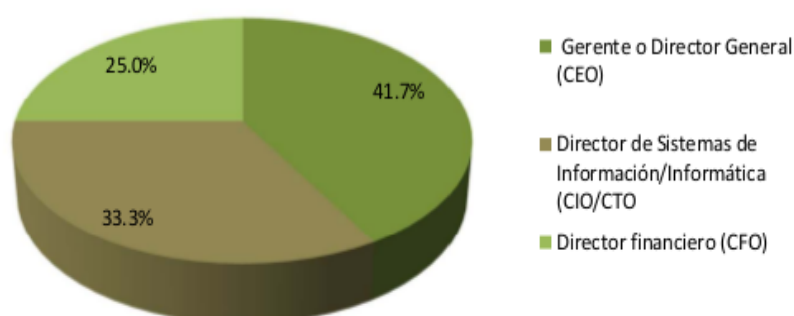
8.2 Herramientas para la implementación y gestión de la Gobernanza de TI

¿Qué marcos de trabajo o herramientas conoce para la implementación y gestión de la Gobernanza de TI?

Herramientas para la implementación de la gobernanza de TI	% de casos
ITIL/ ISO 2000	26,6%
Soluciones de organizaciones profesionales locales o nacionales	16,0%
COBIT	10,7%
Six Sigma	10,7%
Soluciones de organizaciones internacionales.	8,0%
CMM y CMMI	6,7%
PMI, PMIBOK	6,7%
Marco de trabajo desarrollado internamente	6,7%
CISR	2,7%
PRINCE 2	2,7%
Val IT	1,3%
Calder – Moir	1,3%

8.2.1 Participación en la definición de la estructura de Ti para empresas que tienen un marco de trabajo propio

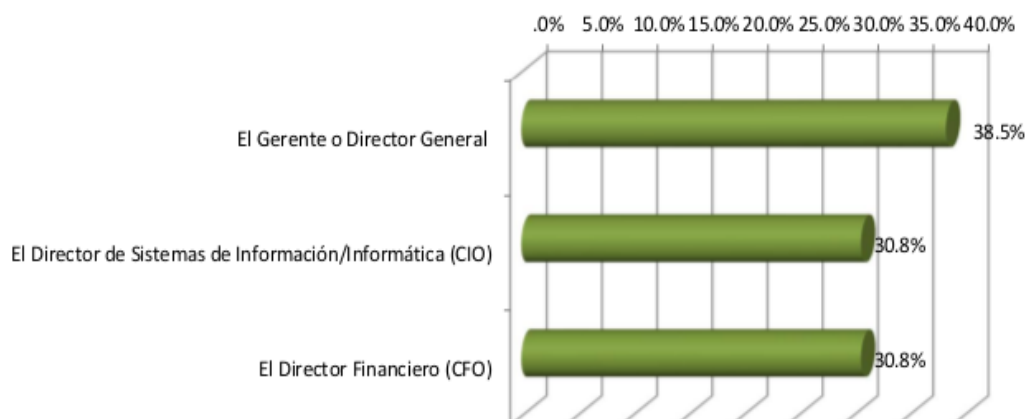
Gráfica 71. Participantes en la definición de la estructura de TI



De aquellas empresas que tienen un marco de trabajo propio (1%), el 41% se caracteriza por ser el director o gerente general quien participe en la definición de la estructura de TI. En el 33% de los casos es el director de sistema de información quien participa de esta definición y en el restante 25% de las empresas es el director financiero quien define esta estructura.

8.2.2 Encargado de la toma de decisiones de Ti para empresas que tienen un marco de trabajo propio

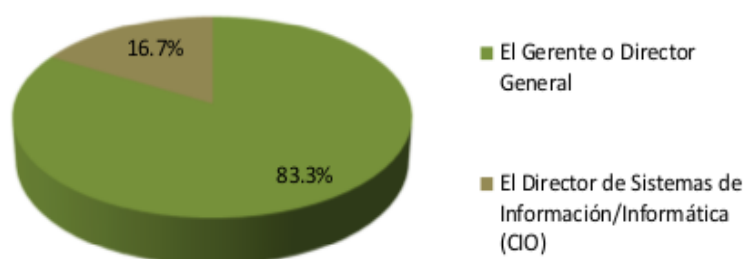
Gráfica 72. Encargado de la toma de decisiones de Ti



En el 38% de estas empresas quien toma las decisiones es el gerente general. En el 30% de las mismas se caracteriza por ser el director de sistemas de información quien realiza esta actividad y el restante 30% de los casos es el director financiero quien se encarga de tomar las decisiones.

8.2.3 Líder de la gobernanza de Ti para empresas que tienen un marco de trabajo propio

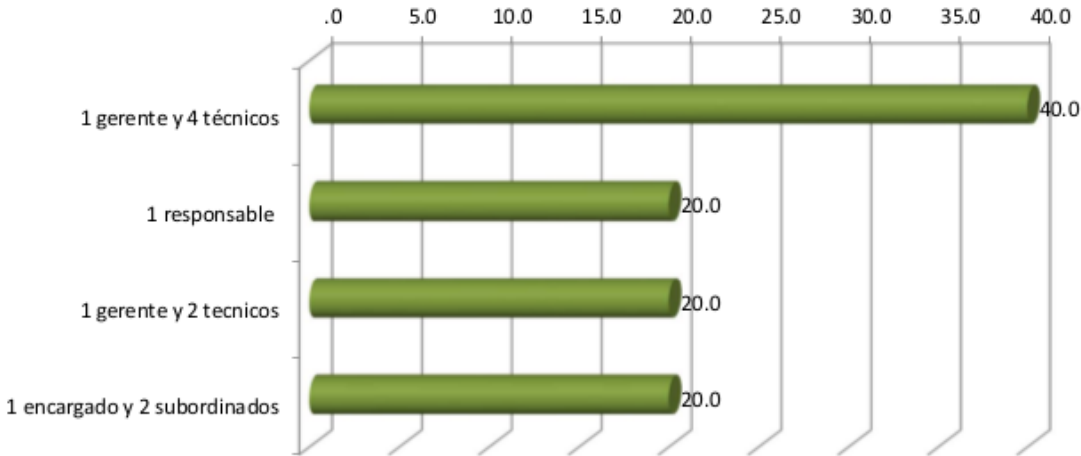
Gráfica 73. Líder de la gobernanza de TI



En el 83% de las empresas que tienen un marco de trabajo propio, quien lidera la gobernanza de TI es el gerente o director general. Y en el 16% de los restantes casos es el director de sistemas de Información/ Informática quien se encarga de liderar la gobernanza.

8.2.4 Roles en la estructura de RRHH de Ti para empresas que tienen un marco de trabajo propio

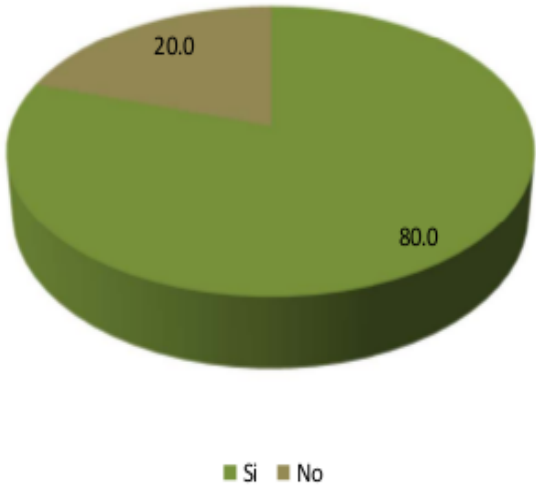
Gráfica 74. Roles en la estructura de RRHH de TI



En el 40% de las empresas que tienen un marco de trabajo propio, la estructura de RRHH de Ti se define por 1 gerente y 4 técnicos .

8.2.5 Existencia de una infraestructura de TI para empresas que tienen un marco de trabajo propio (1% del total de empresas encuestadas)

Gráfica 75. ¿ Tiene una infraestructura de Ti definida en la empresa?



El 80% de las empresas con un marco propio de trabajo se caracterizan por tener un infraestructura de TI definida. El restante 20% de los casos no tiene dicha infraestructura de TI

8.2.6 Cantidad de empleados general y cantidad de empleados de TI para empresas que tienen un marco de trabajo propio

Cantidad de empleados en general	% de casos
90	40,0
18	20,0
35	20,0
50	20,0

El 40% de empresas con un marco propio de trabajo cuenta con 90 empleados.
El 20% tiene 18, 35 y 50 empleados en su empresa.

Cantidad de empleados de TI	% de casos
3	40,0
4	20,0
6	20,0
20	20,0

Respecto a la cantidad de empleados de TI, puede verse que el 40% de las empresas cuenta con 3 y el 20% se caracteriza por tener 4, 6 y 20 empleados de TI trabajando en la empresa.

ANEXO V - Características y estado de la Gestión del Conocimiento en las PYMES del Uruguay

Investigación para Master en Ingeniería en Investigación – Universidad ORT

Lic. Sebastián Ayala

Montevideo, Uruguay

Abril de 2014

Contenido

0 Objetivos y metodología

1 Caracterización de la muestra

2 La gestión del conocimiento en la estrategia de la empresa

3 Etapas de la gestión del conocimiento realizadas en la empresa

4 Herramientas y técnicas de la gestión del conocimiento utilizadas en la empresa

5 Dimensiones de gobierno, evaluación y respuestas del riesgo en TI

6 Factores de éxito y obstáculos de la gestión de conocimiento en su empresa

7 Conclusiones

0. Objetivos y metodología

1. FUNDAMENTACIÓN DEL ESTUDIO

- ✓ *La presente propuesta de investigación se dirige a obtener una aproximación a **perfil, características y estado en materia de Gestión del Conocimiento en PYMES del Uruguay.***
- ✓ *El estudio se realiza en el marco del proceso de elaboración de Tesis de Maestría del Licenciado Sebastián Ayala, en su línea de investigación dedicada al uso de TICs en pequeñas y medianas empresas de nuestro país, y en particular la gestión del conocimiento que en este tipo de empresas se desarrolla.*

2. GESTIÓN DEL CONOCIMIENTO: ¿Qué es? ¿Para qué sirve?

- ✓ *Gestionar el conocimiento consiste en **asegurar la generación constante de nuevos saberes.***
- ✓ *La gestión eficaz del conocimiento en las pymes y la capacidad de éstas para **aprender más rápido** que sus rivales y **optimizar ese conocimiento**, se ha convertido en un **recurso estratégico y diferencial** que, mediante una gestión más eficaz y eficiente, le aporta una indudable **ventaja competitiva.***

3. OBJETIVOS DE INFORMACIÓN

La presente investigación se dirige al cumplimiento de los siguientes objetivos:

PERFIL, CARACTERÍSTICAS Y ACTIVIDADES DE GESTIÓN DEL CONOCIMIENTO EN PYMES DE URUGUAY

Relevar a nivel de un grupo de pequeñas y medianas empresas (PYMES) de ciertos sectores de producción y servicios en Uruguay, acerca de:

- *Perfil y características de PYMES en materia de Gestión del Conocimiento dentro (socios, empleados, colaboradores) y fuera (clientes, proveedores, competidores, mercado en general) de las organizaciones relevadas.*
 - *Recursos humanos e inversión temporal y financiera destinados en actividades de Gestión del Conocimiento.*
 - *Principales políticas y prácticas en Gestión del Conocimiento que se definen desde la Dirección y/o responsable de Área TICs de las PYMES consultadas.*
 - *Principales actividades de Gestión del Conocimiento que se realizan internamente y externamente en las empresas relevadas, periodicidad con que se realizan, destinatarios.*
-

4. METODOLOGÍA DE INVESTIGACIÓN

El estudio prevé la aplicación de una metodología cuantitativa de investigación basada en encuestas telefónicas a Directores y/o responsables de TI en PYMES seleccionadas.

▪ Tipo de estudio

Encuesta Telefónica a Directores y/o Responsables de Área TI en PYMES de ciertos sectores de actividad de interés.

Total de casos: 30 (5 casos por sector)

Muestreo teórico no probabilístico

Sectores de actividad de interés: Financiero, Salud, Tecnología, Infraestructura&Logística, Educación, Agropecuario

De acuerdo al Criterio de Clasificación de Empresas en el Uruguay (según lo establecido en el Decreto N° 504/07 del 20 de diciembre del 2007), según cantidad de personal empleado:

Pequeña Empresa: 5 a 19 personas

Mediana Empresa: 20 a 99 personas

5. ASPECTOS METODOLÓGICOS Y OPERATIVOS

Duración de aplicación de encuesta: 9 minutos.

Extensión de Formulario: 20 preguntas, más 5 preguntas de caracterización de empresas.

Tipo de encuesta: Encuesta Telefónica

Muestreo: Teórico, no probabilístico

Sujeto encuestado: Director y/o Responsable de TI en PYMES seleccionadas teóricamente, instaladas en Montevideo y algunos departamentos representativos del Interior del país (Canelones, Maldonado, Paysandú, Salto).

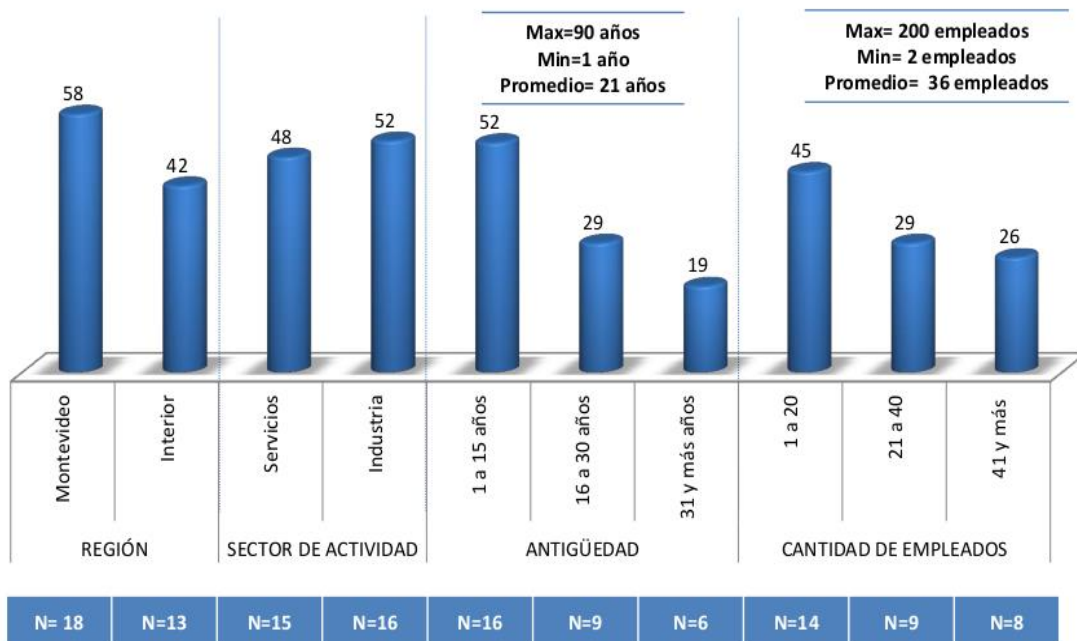
Marco muestral: Listado de 30 PYMES con contactos, proporcionado por contratante. Se ampliará dicho marco muestral con bases de PYMES en Uruguay pertenecientes a los sectores de actividad de interés.

1. Caracterización de la muestra

Gráfico 1. Caracterización de la muestra.

Segmentos: P.4 Sector de actividad de la empresa, P.5 Antigüedad, P.6. Departamento, P.7. Cantidad de empleados

N=31 Total de Encuestados

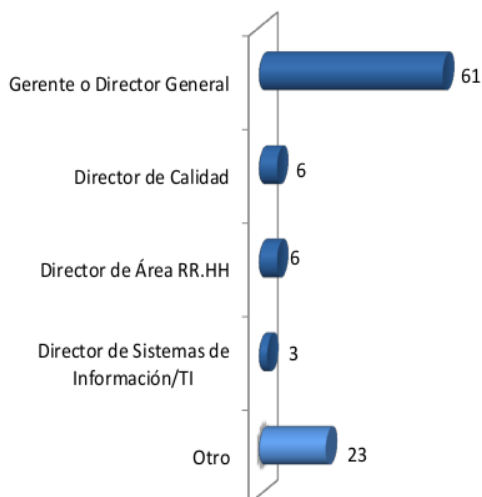


La muestra incluyó un 58% de empresas de Montevideo y un 48% del sector de actividad industrial. La mayor parte de las empresas tendrían entre 1 y 15 años de antigüedad y entre 1 y 20 empleados.

Gráfico 2. Cargo desempeñado por el encuestado
P3. ¿Qué cargo desempeña dentro de su empresa?

Tabla 1. Cargo desempeñado por el encuestado
P3. ¿Qué cargo desempeña dentro de su empresa?
Otros.

N=31 Total de Encuestados



OTROS CARGOS
JEFA DE DPARTAMENTO CONTABLE
GERENTE COMERCIAL
ENCARGADA DE ADMINISTRACIÓN
DIRECTOR FINANCIERO
CONTADOR
AUX ADM CONTABLE RECURSOS HUMANOS
ADMINISTRATIVO

Mayoritariamente la muestra estuvo compuesta por gerentes o directores generales. De todas maneras, se accedió también a distintos tipos de directores y jefes, aunque de secciones más específicas.

Tablas 2 y 3. Sector de actividad de cada PYME
 Segmentos: P.4 Sector de actividad de la empresa

N=31 Total de Encuestados

INDUSTRIA
OPTICA Y LENTES DE CONTACTO
TRABAJO EN FIBRA DE VIDRIO
METALÚRGICA
PRODUCTOS AGROVETERINARIOS
TECNOLOGÍAS (RADIOGRAFÍAS INDUSTRIALES, PRODUCTOS A NIVEL INDUSTRIAL), PARTE DE CONTROL DE CALIDAD
INFRAESTRUCTURA
MAQUINARIA FORESTAL Y AGRÍCOLA
RURAL
MARROQUINERIA
GRANOSUR, SE DEDICA A LA COMPRA VENTA DE GRANOS, GANADO, CARNE, GESTIÓN DE PLANTAS DE CILOS, Y FLOTA PROPIA DE CAMIONES
LACTEOS
QUIMICA
VESTIMENTA
MICROBIOLOGIA
DROGUERÍA Y DISTRIBUCIÓN DE PRODUCTOS QUÍMICOS.
INFRAESTRUCTURA

SERVICIOS
DESARROLLO WEB
CONSULTORÍA EN RECURSOS HUMANOS Y GERENCIA
COMERCIO
PRESTADORA DE SERVICIOS DE CALIBRACIÓN Y VENTA Y REPARACIÓN DE BALANES INDUSTRIALES
DESARROLLO DE SOFTWARE
SERVICIO DE ACOMPAÑANTES
SERVICIOS EN INGENIERÍA
MEDIOS DE COMUNICACIÓN
SERVICIOS INFOMATICOS
CONSTRUCCIÓN VIAL
SERVICIO TÉCNICO INFORMÁTICO
HOTELERÍA Y GASTRONOMÍA
SALUD
SOPORTE TÉCNICO
INFORMÁTICA

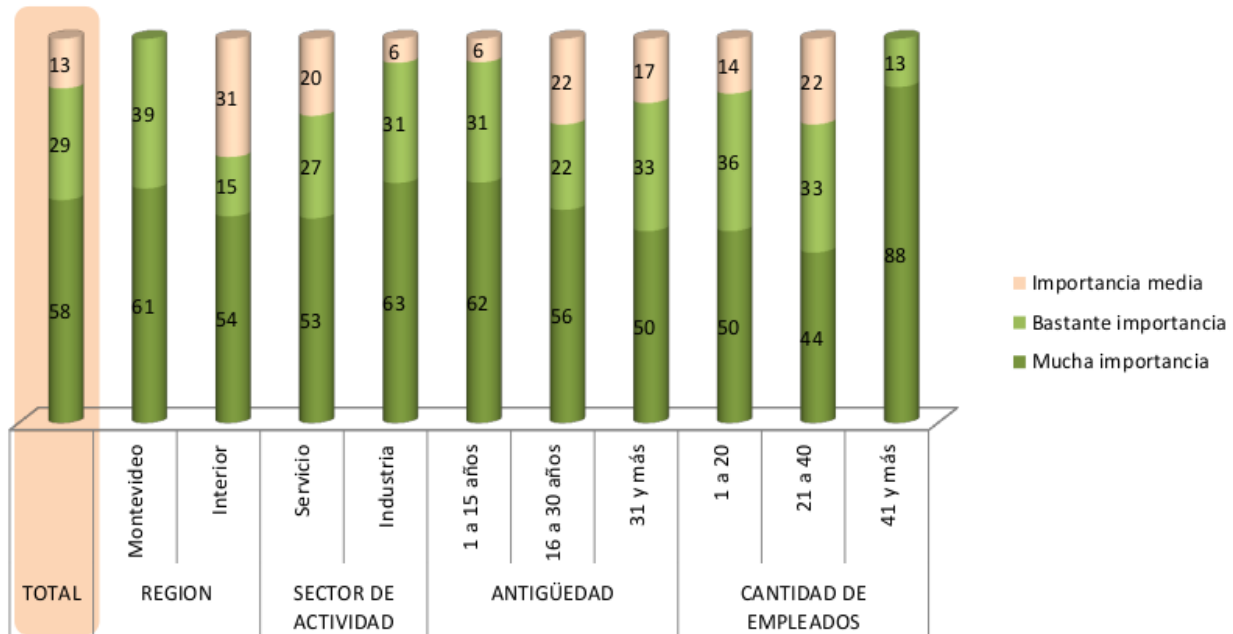
2. La Gestión del Conocimiento en la estrategia de la empresa

Gráfico 1. Importancia de la gestión del conocimiento.

Segmentos: Región, antigüedad, cantidad de empleados, sector de actividad

N=31 Total de Encuestados

P8. ¿Qué importancia considera que tiene la GC como elemento que permite la consecución de la estrategia, misión y visión en su empresa?



La mayoría de los consultados encuentran muy importante la «gestión del conocimiento».

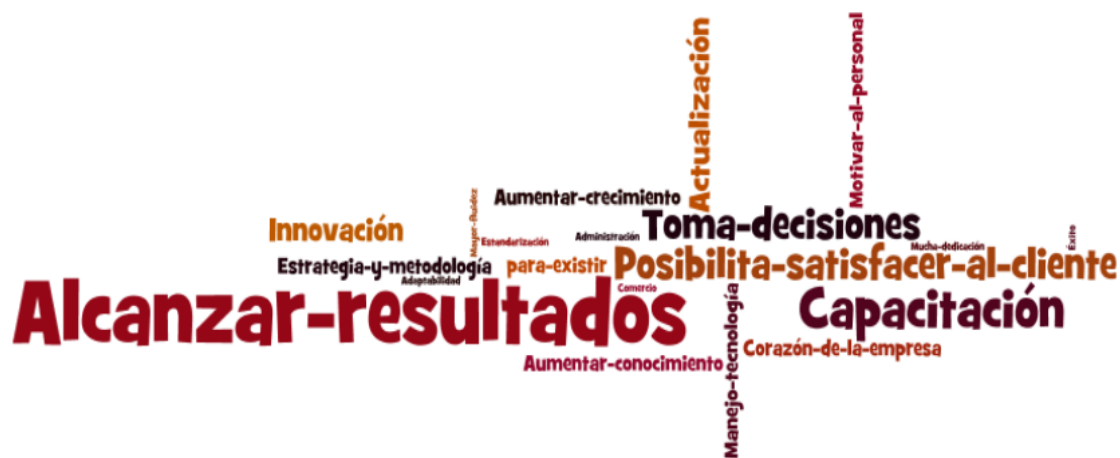
Es en Montevideo y en las empresas de más de 40 empleados que es considerada en mayor medida como un aspecto de gran importancia dentro del desarrollo de una empresa. Sin embargo, puede apreciarse que en el interior del país un 31% de los encuestados encuentra que tiene una importancia media, mientras que en Montevideo el 100% considera que tiene entre mucha y bastante importancia.

Diagrama 1. Motivos de importancia de la gestión del conocimiento.

Pregunta abierta: Nube de palabras

P8. ¿Qué importancia considera que tiene la GC como elemento que permite la consecución de la estrategia, misión y visión en su empresa?

P9. ¿Por qué?



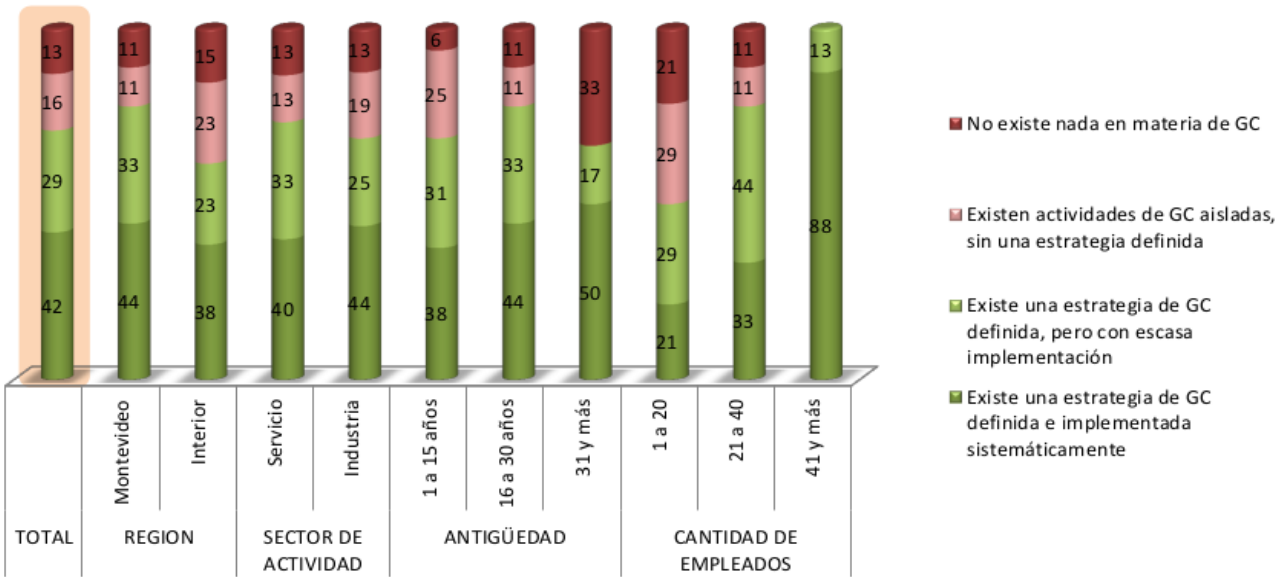
Se destaca especialmente entre los motivos para considerar de mucha importancia a la «gestión del conocimiento» la orientación práctica guiada a resultados. Satisfacer al cliente y mejorar la calidad del producto también están muy presentes y son aspectos relacionados con la idea de alcanzar resultados y metas en forma exitosa. Otro de los aspectos que se destaca es la innovación, que se señala como aspecto central para el desarrollo de nuevos productos y captación de clientes así como también la capacitación de los empleados.

Gráfico 2. Estrategia de gestión de conocimiento utilizada en su organización

Segmentos: Región, antigüedad, cantidad de empleados, sector de actividad

P10 ¿Cuál de las siguientes afirmaciones refleja mejor la estrategia de GC en su organización?

N=31 Total de Encuestados



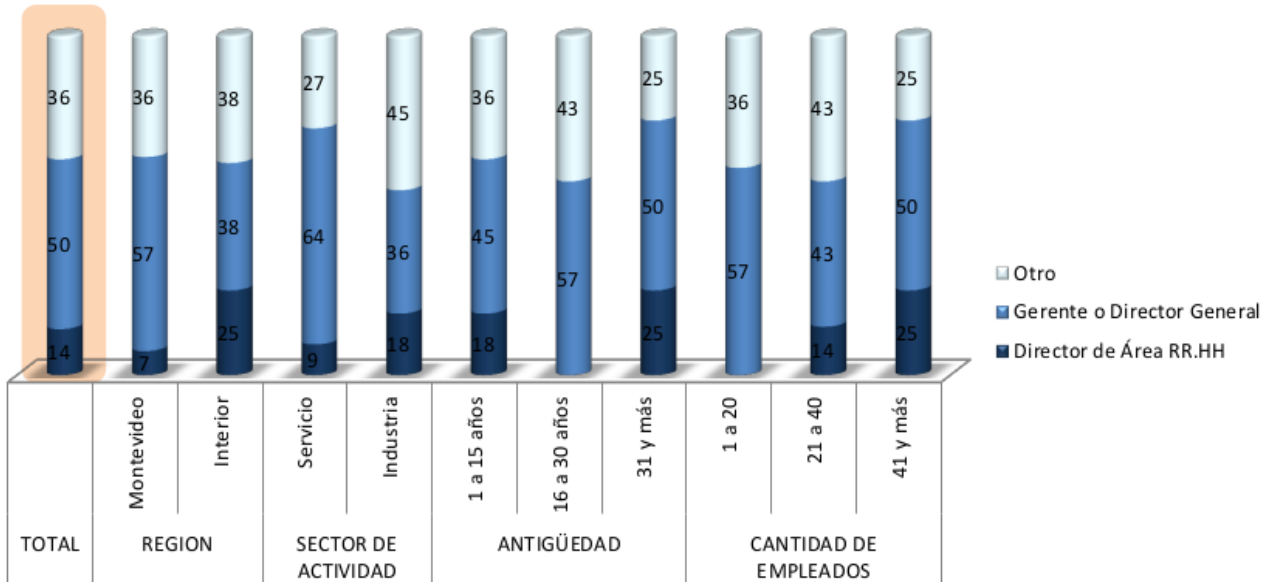
Una mayoría relativa del 42% posee una estrategia implementada y sistematizada respecto a la «gestión del conocimiento» en su empresa. Aún así no existen diferencias significativas entre las distintas categorías de segmentación, a no ser en «cantidad de empleados» donde las empresas mas numerosas se alejan considerablemente de la no existencia de estrategias.

Gráfico 3. Cargos involucrados en la estrategia de gestión de conocimiento

Segmentos: Región, antigüedad, cantidad de empleados, sector de actividad

P11. ¿qué cargos en la organización participan de su definición e implementación? (marcar todas las opciones mencionadas)

N=22 Quienes cuentan con una estrategia de GC definida



En general, los cargos que tendrían más participación en la implementación de las diversas estrategias para la serían los gerentes o directores generales.

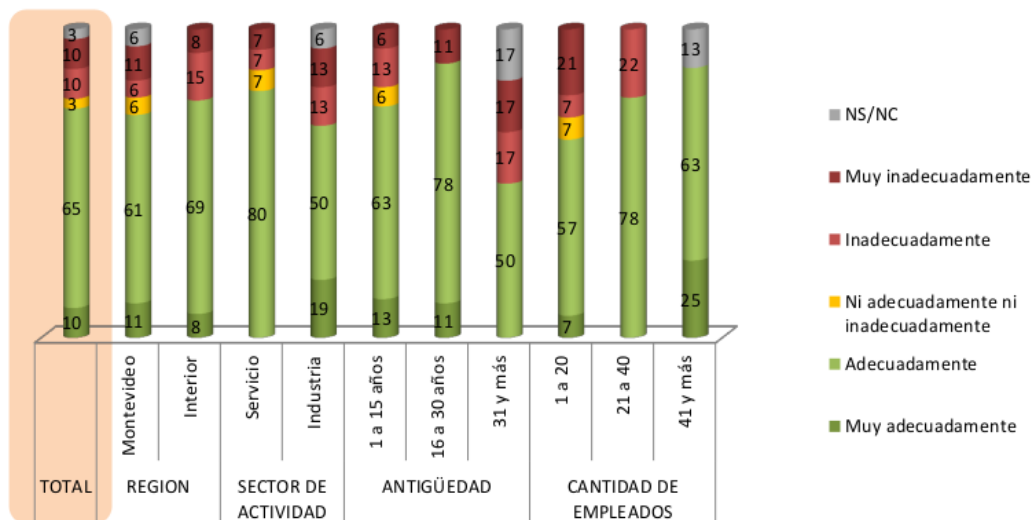
Sucede lo opuesto en el caso de las PYMES del interior del país en las que un 25% de Directores de área de RR.HH participan en la definición e implementación de estrategia y así como también lo hacen un 38% de otros cargos. Para el sector de industrias no es tan destacada, como en el sector servicios la participación de gerentes generales, lo mismo ocurre en las empresas con menos años de trayectoria.

2.1 Etapas de la Gestión del Conocimiento realizadas en la empresa

Gráfico 1. Fase 1: Identificación: determinar dónde está el conocimiento, qué es lo que falta conocer en su organización
Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

N=31 Total de Encuestados

P12. A continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)

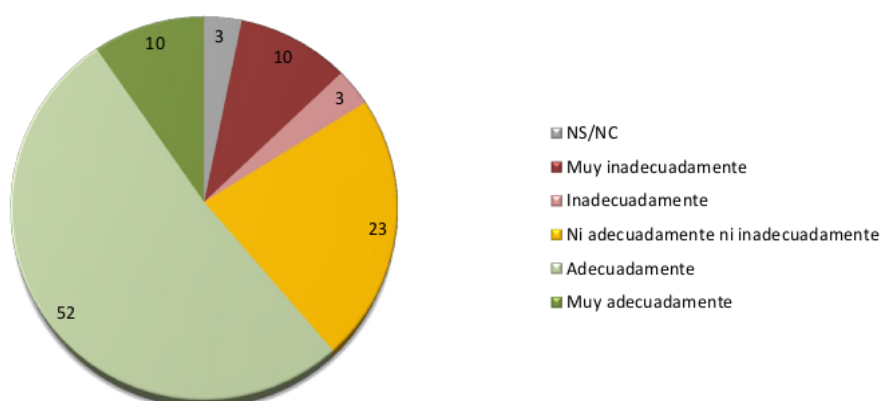


La etapa de identificación, dentro del ciclo de Gestión del Conocimiento, parece desarrollarse en forma muy adecuada en la amplia mayoría de las empresas en las que se realizó la encuesta, de acuerdo con la percepción de los consultados. Asimismo, parecería desarrollarse de mejor manera en las empresas del sector de servicios, de una antigüedad media y mayor cantidad de empleados.

Gráfico 2. Fase 2: Adquisición: adquirir el faltante de conocimiento en su organización.
Frecuencia simple.

N=31 Total de Encuestados

P12. A continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)



El proceso de adquisición del faltante conocimiento de la organización es una practica evaluada por los encuestados como adecuada o muy adecuada, de acuerdo a como se realiza en sus empresas (62%). Cabe destacar que un 13% señala que se realiza en forma inadecuada y muy inadecuada.

Tabla 1. Fase 2: Adquisición: adquirir el faltante de conocimiento en su organización.

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P12. A continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)

	TOTAL	REGION		SECTOR DE ACTIVIDAD		ANTIGÜEDAD			CANTIDAD DE EMPLEADOS		
		Montevideo	Interior	Servicio	Industria	1 a 15 años	16 a 30 años	31 y más	1 a 20	21 a 40	41 y más
Muy adecuadamente	10	17	-----	7	13	13	11	-----	14	-----	13
Adecuadamente	52	50	54	60	44	56	56	33	36	56	75
Ni adecuadamente ni inadecuadamente	23	17	31	20	25	19	11	50	29	33	-----
Inadecuadamente	3	6	-----	7	-----	-----	11	-----	-----	11	-----
Muy inadecuadamente	10	6	15	7	13	13	11	-----	21	-----	-----
NS/NC	3	6	-----	-----	6	-----	-----	17	-----	-----	13

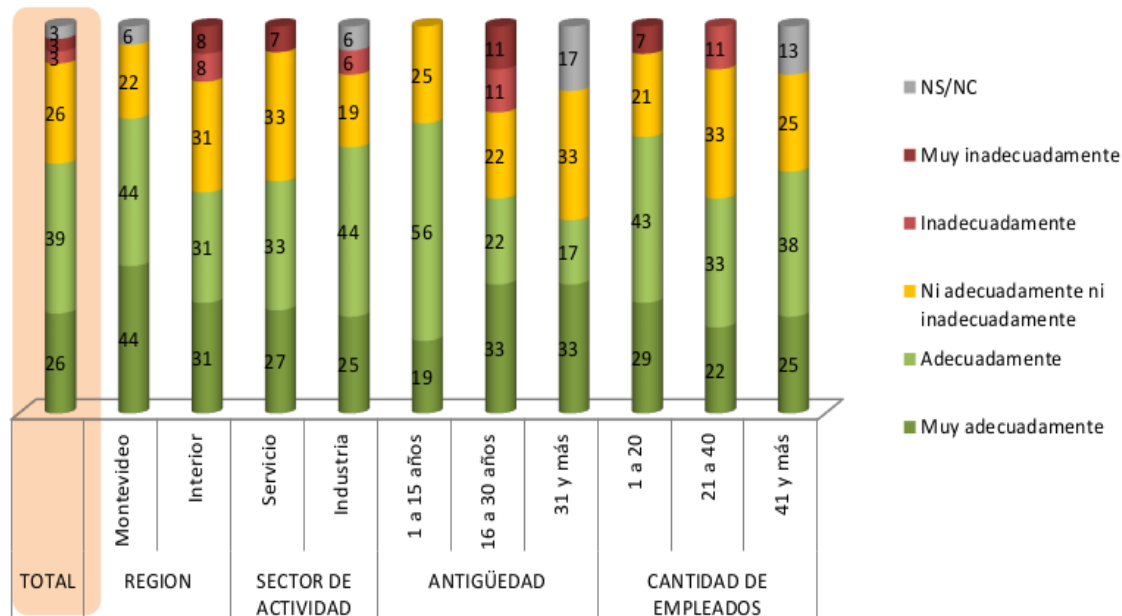
Observando la variable de acuerdo a distintas variables de segmentación se destaca que quienes en mayor medida señalar que la etapa de adquisición del conocimiento se realiza en forma adecuada y muy adecuada son las PYMES de Montevideo, del sector servicios y con antigüedad mayor a 40 años. Las empresas de menor tamaño son las que en mayor medida califican al proceso como muy inadecuado.

Gráfica 3. Fase 3: Desarrollo: desarrollar nuevas habilidades, productos o ideas en su organización

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P12. A continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)

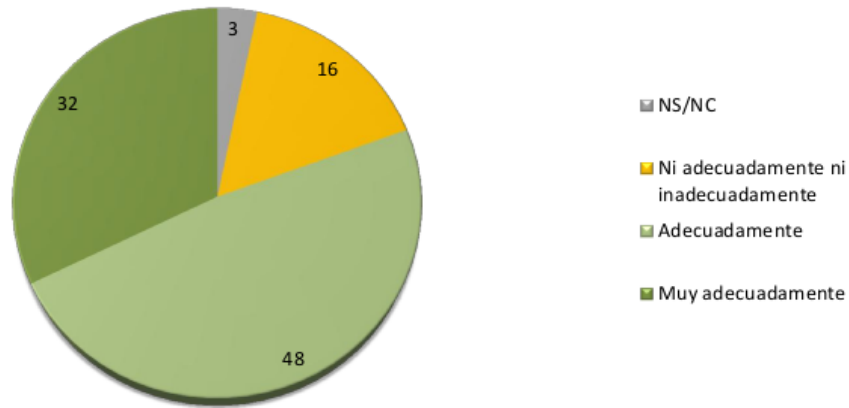


En lo que respecta a la etapa de desarrollo, el 65% considera que en su empresa esta fase se realiza de manera adecuada o muy adecuada. Esta percepción es especialmente sostenida por las empresas más nuevas, las de Montevideo y del sector industrial.

Gráfica 4. Fase 4: Compartir o distribuir el conocimiento: intercambiar el conocimiento disponible a quien lo requiera
Frecuencia simple.

N=31 Total de Encuestados

P12. A continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)



La fase referida a compartir o distribuir el conocimiento de la empresa encuentra tal vez los mejores niveles de implementación por parte de los encuestados, ya que el 80% considera que su empresa lo implementa de manera adecuada o muy adecuada. Asimismo, cabe señalar que ningún encuestado utiliza la categoría de respuesta intermedia para evaluar este ítem.

Tabla 2. Fase 4: Compartir o distribuir el conocimiento: intercambiar el conocimiento disponible a quien lo requiera Segmentos: Región, sector de actividad, antigüedad y cantidad de empleados.

N=31 Total de Encuestados

P12. A continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)

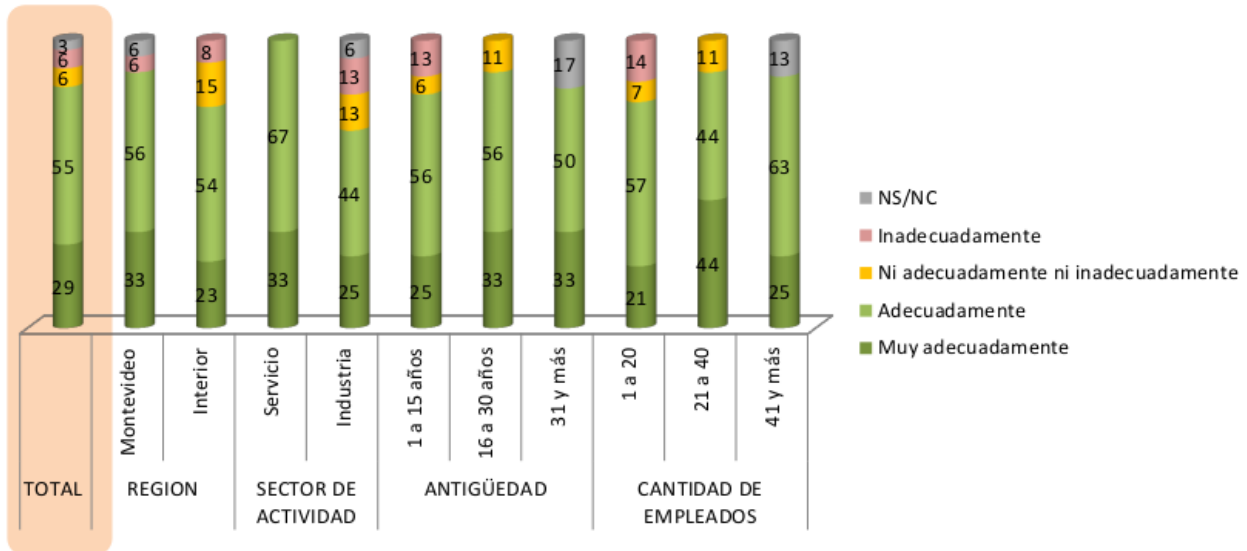
	TOTAL	REGION		SECTOR DE ACTIVIDAD		ANTIGÜEDAD			CANTIDAD DE EMPLEADOS		
		Montevideo	Interior	Servicio	Industria	1 a 15 años	16 a 30 años	31 y más	1 a 20	21 a 40	41 y más
Muy adecuadamente	32	28	38	20	44	38	22	33	43	22	25
Adecuadamente	48	50	46	67	31	38	78	33	29	67	63
Ni adecuadamente ni inadecuadamente	16	17	15	13	19	25	-----	17	29	11	-----
NS/NC	3	6	-----	-----	6	-----	-----	17	-----	-----	13

Las PYMES del interior, orientadas a servicios y que se encuentran entre los 16 y 30 años son las que tienden a aplicar el intercambio del conocimiento en mayor medida en forma más adecuada. Si se considera solo la categoría «muy adecuadamente» se puede ver que las empresas con menos cantidad de empleados son quienes comparten y distribuyen el conocimiento de mejor manera, mientras que ocurre lo opuesto en las empresas de mayor cantidad de empleados. Los mayores niveles de desconocimiento se identifican en las empresas más antiguas.

Gráfica 5. Fase 5: Uso del conocimiento: hacer uso del conocimiento en aplicaciones concretas para su organización.
Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

N=31 Total de Encuestados

P12. A continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)

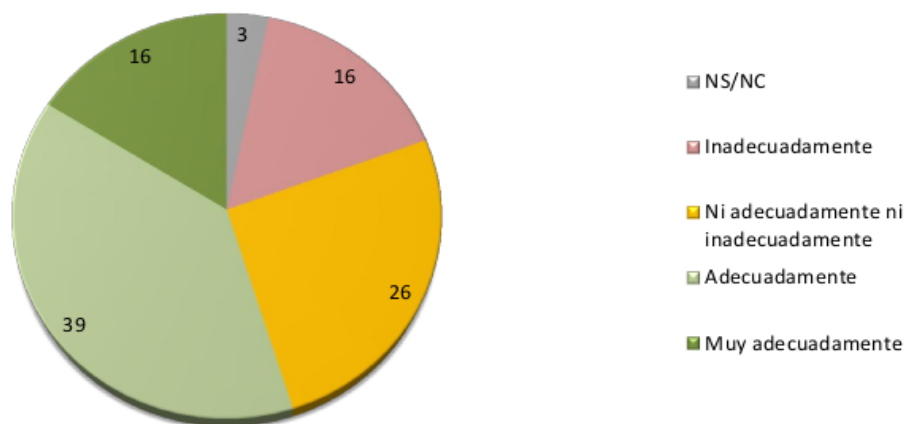


Mayoritariamente, el hacer uso del conocimiento de forma concreta a través de aplicaciones específicas es evaluado, mayoritariamente como una fase que se realiza de manera adecuada. Las PYMES orientadas a servicios son las que presentan los mejores niveles de evaluación en este sentido. También se destacan las empresas de mayor antigüedad, las de Montevideo y las que tienen mayor cantidad de empleados.

Gráfica 6. Fase 6: Retención del conocimiento: almacenamiento y actualización del conocimiento
Frecuencia simple.

N=31 Total de Encuestados

P12. A continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)



La mayoría de los encuestados, 55%, declara que la fase de retención del conocimiento en su organización se realiza en forma muy adecuada y adecuada. Mientras un 16% declara que se realiza en forma inadecuada.

Tabla 3. Fase 6: Retención del conocimiento: almacenamiento y actualización del conocimiento
Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

N=31 Total de Encuestados

P12. A continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)

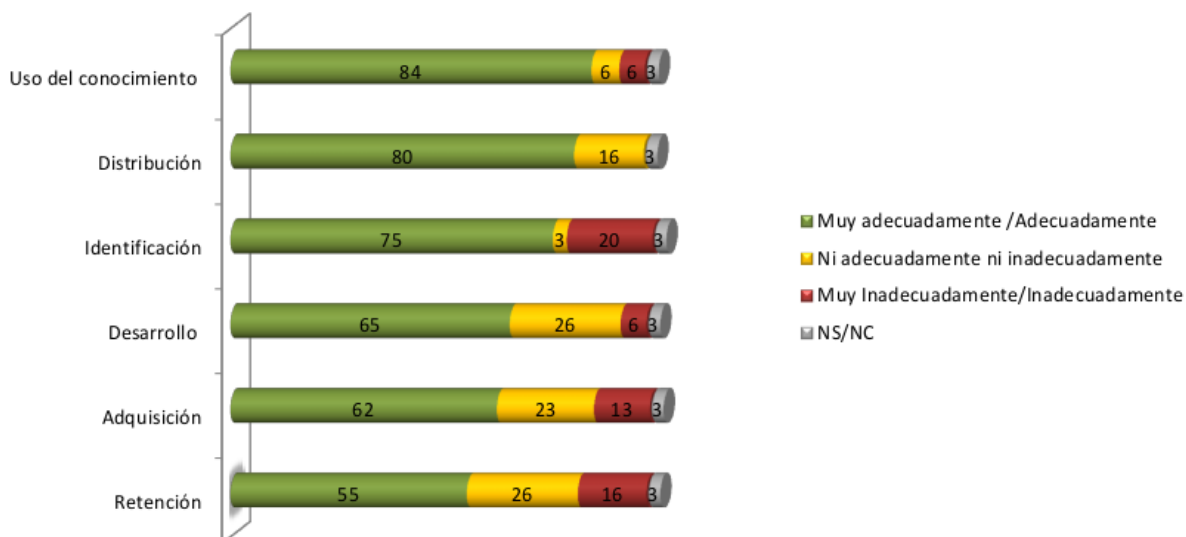
	TOTAL	REGION		SECTOR DE ACTIVIDAD		ANTIGÜEDAD			CANTIDAD DE EMPLEADOS		
		Montevideo	Interior	Servicio	Industria	1 a 15 años	16 a 30 años	31 y más	1 a 20	21 a 40	41 y más
Muy adecuadamente	16	17	15	20	13	19	11	17	14	22	13
Adecuadamente	39	39	38	33	44	31	67	17	36	33	50
Ni adecuadamente ni inadecuadamente	26	28	23	33	19	38	11	17	29	22	25
Inadecuadamente	16	11	23	13	19	13	11	33	21	22	-----
NS/NC	3	6	-----	-----	6	-----	-----	17	-----	-----	13

Quienes en mayor medida señalan que la fase de retención de realiza de manera muy adecuada serían aquellas de entre 21 y 40 empleados. En el extremo opuesto, quienes en mayor medida consideran que se implementa de manera inadecuada, serían las empresas de mayor antigüedad, que es donde también se identifican los mayores niveles de desconocimiento.

Gráfica 7. Grafico resumen: Fases principales del ciclo de gestión del conocimiento.

N=31 Total de Encuestados

P12. Continuación vamos a mencionarle 6 etapas o fases principales que describen el ciclo de la GC en una organización, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las realiza su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente)



En general, para todas las fases que describen el ciclo de gestión del conocimiento, se registran mayoritariamente valores muy adecuados y adecuados. Igualmente cabe destacar que un 20% de los encuestados dice que la etapa de identificación se realiza en forma «muy inadecuada» o «inadecuada». Así como también ocurre con la etapa de retención, que un 16% de los encuestados señala que se realiza en forma «muy inadecuada» o «inadecuada».

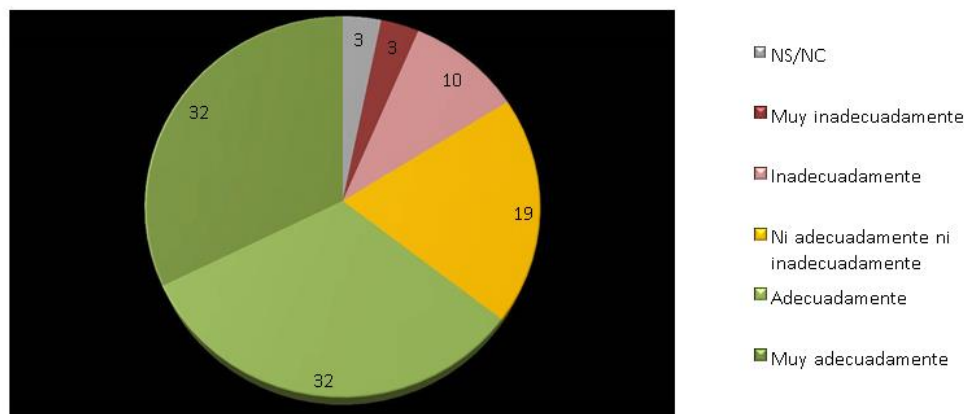
2.2 Herramientas y técnicas de la Gestión del Conocimiento utilizadas en la empresa

Gráfica 1. ACCESIBILIDAD: Que el conocimiento esté disponible para quien lo necesite

N=31 Total de Encuestados

Frecuencia simple.

P13. A continuación vamos a mencionarle una serie de herramientas y técnicas de GC, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las aplica su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente, 5=Muy inadecuadamente).



La mayoría de las empresas declaran aplicar la accesibilidad del conocimiento de manera adecuada o muy adecuada. Sin embargo, es de destacar que un 19% de los encuestados resalta no implementar esta herramienta de manera «ni adecuada ni inadecuadamente» y un 13% resalta hacerlo de forma «inadecuada» y «muy inadecuada».

Tabla 2. ACCESIBILIDAD: Que el conocimiento esté disponible para quien lo necesite

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P13. A continuación vamos a mencionarle una serie de herramientas y técnicas de GC, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las aplica su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).

	TOTAL	REGION		SECTOR DE ACTIVIDAD		ANTIGÜEDAD			CANTIDAD DE EMPLEADOS		
		Montevideo	Interior	Servicio	Industria	1 a 15 años	16 a 30 años	31 y más	1 a 20	21 a 40	41 y más
Muy adecuadamente	32	28	38	33	31	44	22	17	43	22	25
Adecuadamente	32	33	31	40	25	19	56	33	21	33	50
Ni adecuadamente ni inadecuadamente	19	28	8	20	19	25	-----	33	21	22	13
Inadecuadamente	10	6	15	7	13	13	11	-----	14	11	-----
Muy inadecuadamente	3	-----	8	-----	6	-----	11	-----	-----	11	-----
NS/NC	3	6	-----	-----	6	-----	-----	17	-----	-----	13

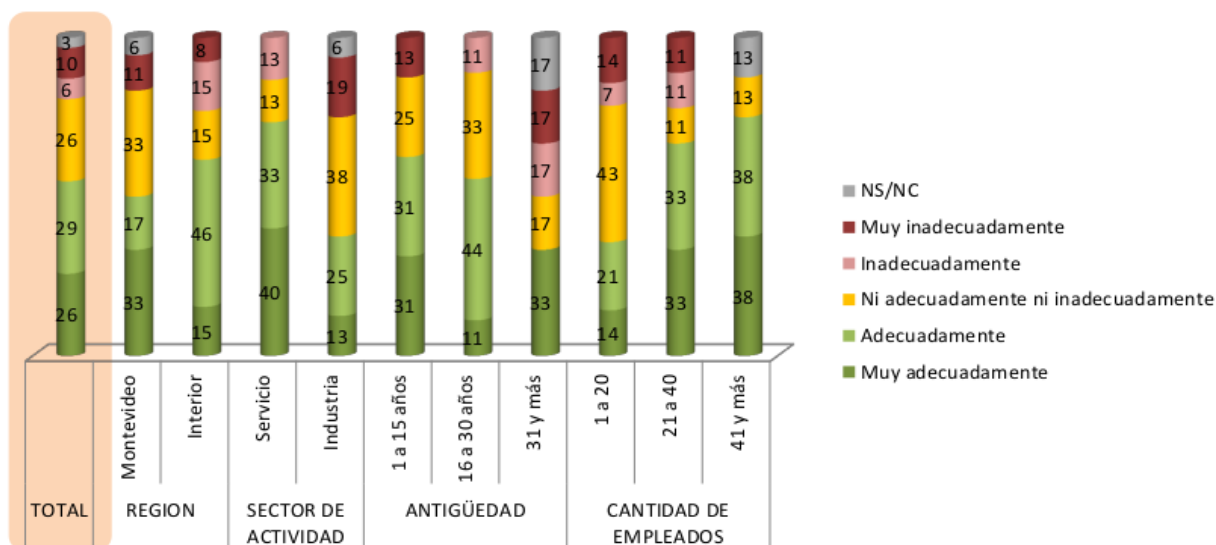
Quienes evalúan la aplicación de la accesibilidad de manera muy adecuada son en mayor medida las empresas más nuevas y aquellas con menor cantidad de empleados. Se identifica que el mayor nivel de desconocimiento se destaca entre las empresas más antiguas, como ya se ha identificado previamente.

Gráfica 2. MEMORIA ORGANIZACIONAL: almacenamiento de la info. en forma de repositorio permanente; consulta y análisis de bases de datos, publicaciones etc.

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P13. A continuación vamos a mencionarle una serie de herramientas y técnicas de GC, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las aplica su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).



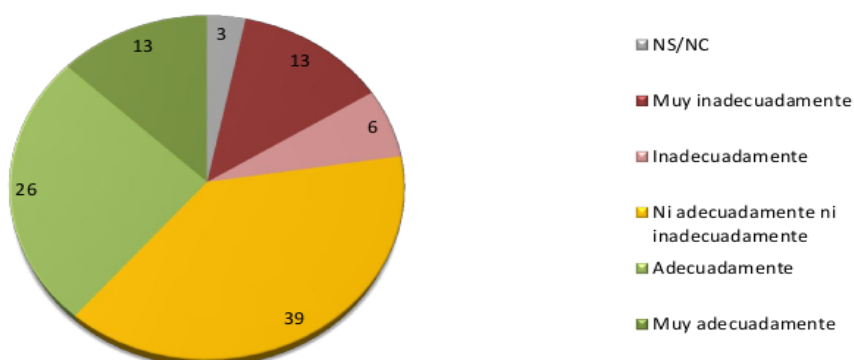
El 55% de las PYMES declaran poseer un manejo adecuado o muy adecuado de la memoria organizacional. Las PYMES de servicios, con más de 40 empleados sobresalen en mayor medida respecto a las herramientas de memoria institucional, siendo las que mejor evalúan este atributo.

Gráfica 3. GRUPOS EXPERTOS Y CÍRCULOS DE CALIDAD: grupos de personas en la empresa o asesores externos que regularmente trabajan en la mejora y aprendizaje organizacional

N=31 Total de Encuestados

Frecuencia Simple.

P13. A continuación vamos a mencionarle una serie de herramientas y técnicas de GC, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las aplica su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).



Se identifican dos grandes grupos de empresas, por un lado, el 39% de las consultadas evalúan que la gestión del conocimiento en lo que refiere a grupos externos y círculos de calidad se realiza de manera adecuada o muy adecuada. Por otro lado, también un 39% señala que se gestiona de manera ni adecuada ni inadecuada.

Tabla 3. GRUPOS EXPERTOS Y CÍRCULOS DE CALIDAD: grupos de personas en la empresa o asesores externos que regularmente trabajan en la mejora y aprendizaje organizacional

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P13. A continuación vamos a mencionarle una serie de herramientas y técnicas de GC, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las aplica su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).

	TOTAL	REGION		SECTOR DE ACTIVIDAD		ANTIGÜEDAD			CANTIDAD DE EMPLEADOS		
		Montevideo	Interior	Servicio	Industria	1 a 15 años	16 a 30 años	31 y más	1 a 20	21 a 40	41 y más
Muy adecuadamente	13	17	8	20	6	13	11	17	7	22	13
Adecuadamente	26	22	31	27	25	38	22	0	21	22	38
Ni adecuadamente ni inadecuadamente	39	39	38	40	38	31	56	33	50	22	38
Inadecuadamente	6	-----	15	7	6	6	11	-----	7	11	-----
Muy inadecuadamente	13	17	8	7	19	13	-----	33	14	22	-----
NS/NC	3	6	-----	-----	6	-----	-----	17	-----	-----	13

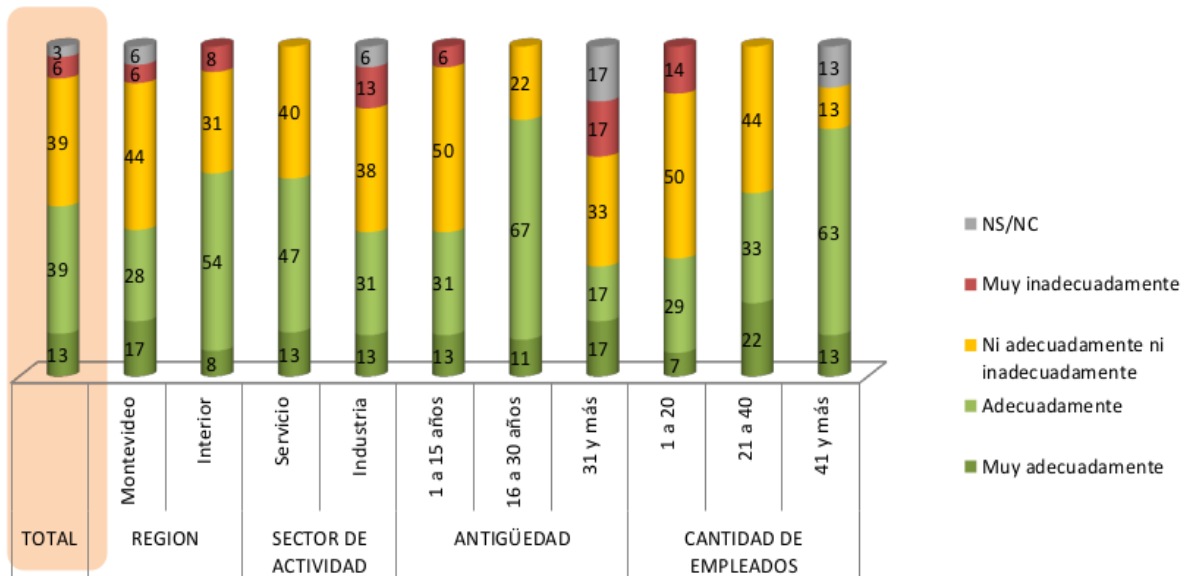
Se identifica que son las empresas de mayor antigüedad en si funcionamiento y con una cantidad media de empleados las que en mayor medida juzgan como inadecuada su gestión en lo que refiere a este atributo.

Gráfica 4. LECCIONES APRENDIDAS Y MEJORES PRÁCTICAS: registro de lo aprendido para su uso posterior y registro de mejores formas de hacer las tareas

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P13. A continuación vamos a mencionarle una serie de herramientas y técnicas de GC, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las aplica su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).



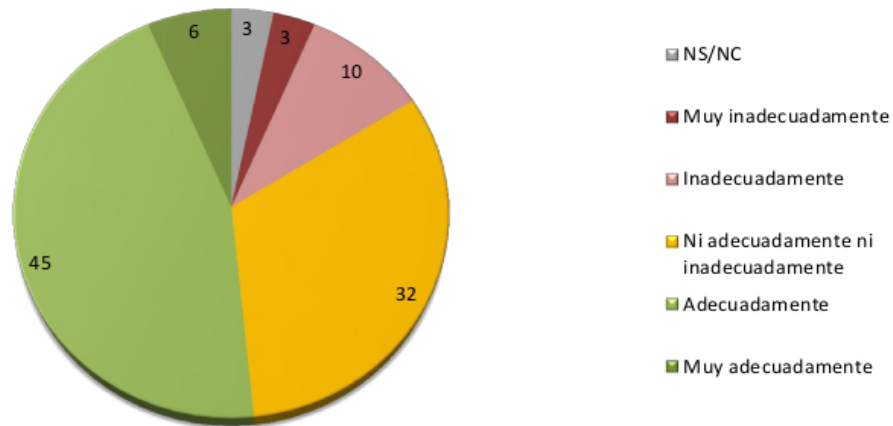
Son mayoría las PYMES que realizan una adecuada o muy adecuada implementación de las lecciones aprendidas (52%), a ún así, la categoría más neutral acumula un considerable porcentaje (39%). Las empresas de 16 a 30 años y las de mas de 41 empleados son las que cuentan con mayor porcentajes de «adecuadamente»

Gráfica 5. PLANES DE FORMACIÓN Y CAPACITACIÓN INTERNA/EXTERNA

N=31 Total de Encuestados

Frecuencia Simple.

P13. A continuación vamos a mencionarle una serie de herramientas y técnicas de GC, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las aplica su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).



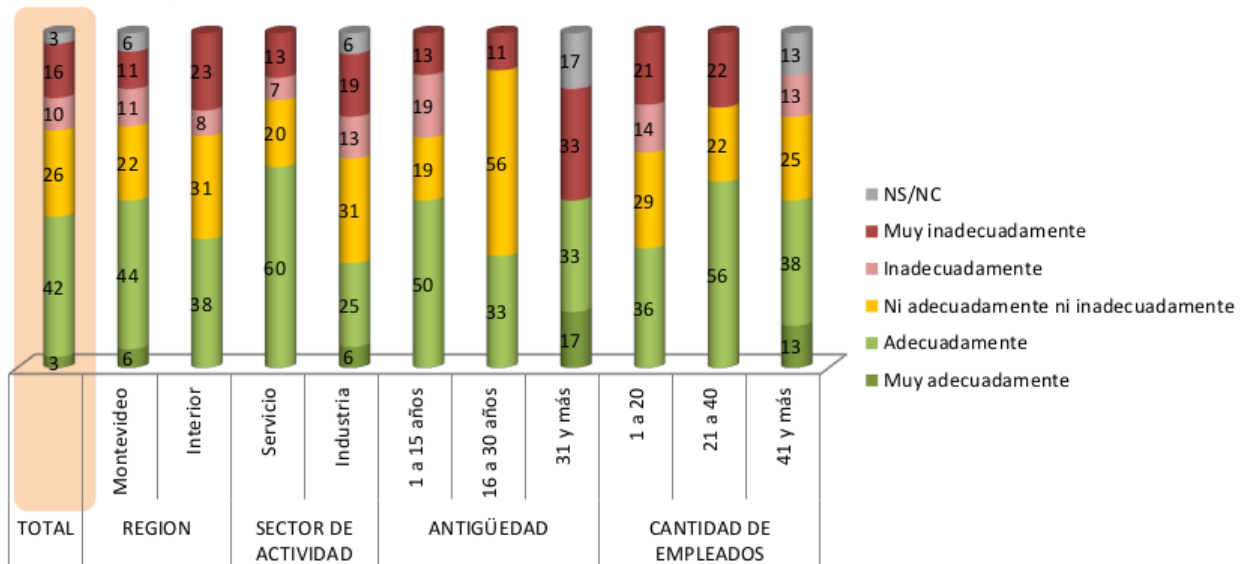
Los planes de formación y capacitación se llevan a cabo de forma más bien adecuada, esto es lo que plantea el 45% de los encuestados. De todas maneras, cabe destacar que la neutralidad ante este aspecto también es relevante (32%). Se resalta también un 13% que dice aplicar esta herramienta en forma «inadecuada» y «muy inadecuada».

Gráfica 6. CLASIFICACIÓN Y CLUSTERING: ordenar y agrupar el conocimiento en determinados grupos de interés o temas, para facilitar su acceso a quien deba tenerlo

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P13. A continuación vamos a mencionarle una serie de herramientas y técnicas de GC, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las aplica su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).

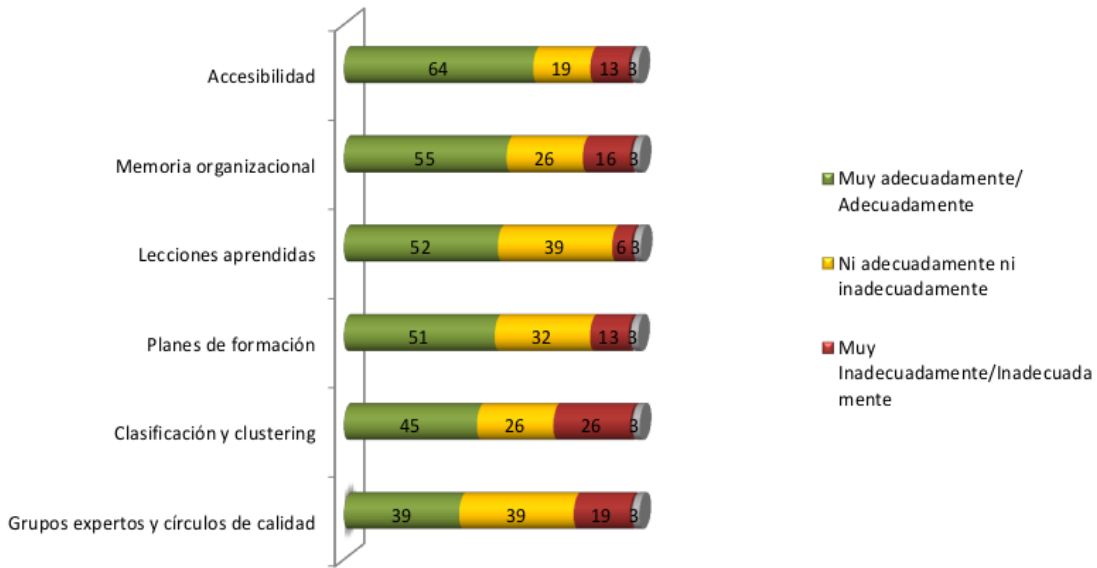


Un 45% de los encuestados, sostiene que realizan en sus organizaciones un manejo «muy adecuado» y «adecuado» de la herramienta de «clasificación y clustering». Esto se da en mayor medida entre las PYMES de Montevideo, las que se desarrollan en el sector de servicios y las que tienen entre 21 y 40 empleados.

Gráfica 7. Gráfico resumen: Herramientas y técnicas.

N=31 Total de Encuestados

P13. A continuación vamos a mencionarle una serie de herramientas y técnicas de GC, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las aplica su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).



En general, se registran valores de adecuación superiores al 50% para la mayor parte de las herramientas y técnicas de Gestión del Conocimiento evaluadas. Sin embargo para el caso de lecciones aprendidas clasificación y clustering se identifica el mayor porcentaje de evaluación negativa.

2.3 Dimensiones de gobierno, evaluación y respuesta del riesgo en TI

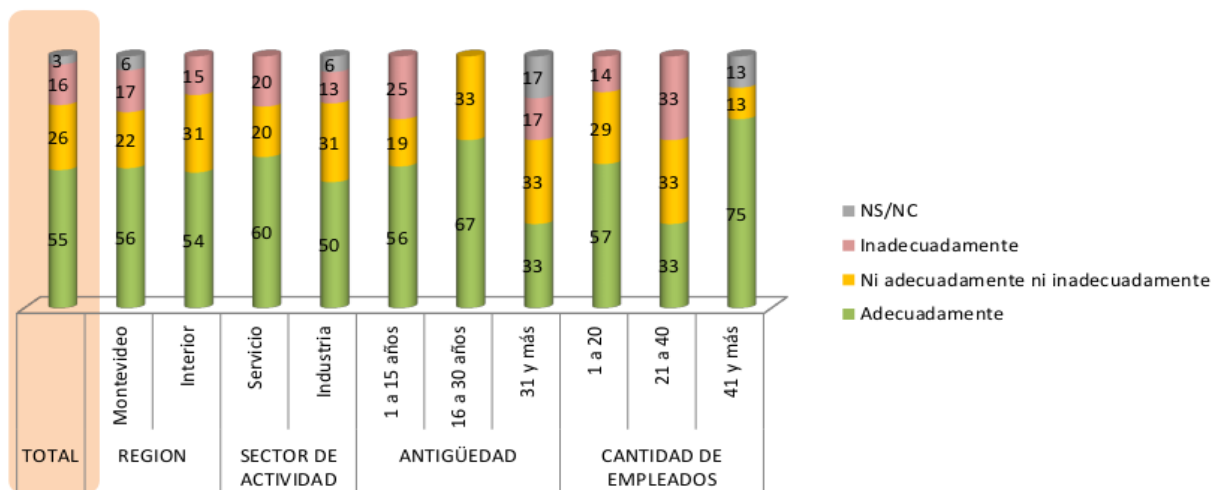
Gráfica 1. GOBIERNO DEL RIESGO EN TI Y GLOBAL.

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P14. A continuación vamos a mencionarle una serie de dimensiones de gobierno, evaluación y respuesta del riesgo en TI, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las gestiona su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).

P14.a. (GOBIERNO DEL RIESGO EN TI y GLOBAL) Visión común del riesgo en toda la organización, integración con la gestión de riesgos integral en la empresa y toma de decisiones del riesgo de negocio



El gobierno del riesgo es percibido por la mayor parte de las empresas como una dimensión que su organización gestiona de manera adecuada. Sin embargo, cabe destacar que el 16% lo evalúa de manera negativa. Este porcentaje se ve especialmente agravado en el caso de las empresas de servicio, de menor antigüedad y con 21 a 40 empleados.

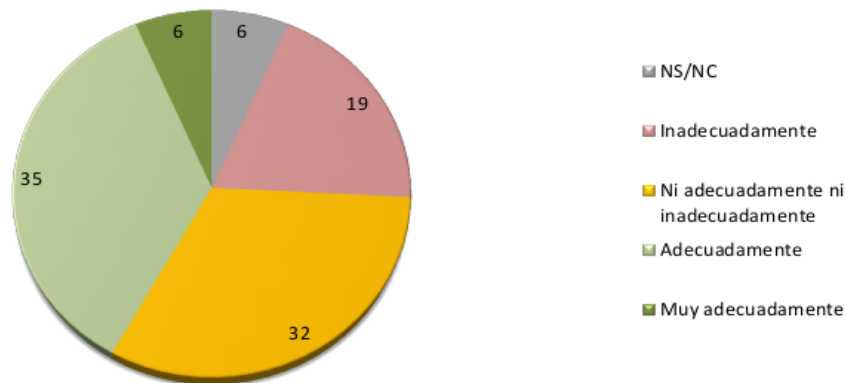
Gráfica 2. EVALUACIÓN DE RIESGO EN TI.

N=31 Total de Encuestados

Frecuencia Simple.

P14. A continuación vamos a mencionarle una serie de dimensiones de gobierno, evaluación y respuesta del riesgo en TI, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las gestiona su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).

P14.b. (EVALUACIÓN DE RIESGO EN TI) Recolección de datos, evaluación de riesgos y mantenimiento del perfil de riesgo en TI en su organización.



La evaluación del riesgo es en gran medida implementada adecuadamente, de acuerdo con las respuestas de los encuestados (41). Igualmente, cabe destacar que se identifican significativos niveles de respuestas intermedias, a través de la utilización de la categoría «Ni adecuada ni inadecuadamente» (32%).

Tabla 1. EVALUACIÓN DE RIESGO EN TI.

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P14. A continuación vamos a mencionarle una serie de dimensiones de gobierno, evaluación y respuesta del riesgo en TI, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las gestiona su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).

P14.b. (EVALUACIÓN DE RIESGO EN TI) Recolección de datos, evaluación de riesgos y mantenimiento del perfil de riesgo en TI en su organización.

	TOTAL	REGION		SECTOR DE ACTIVIDAD		ANTIGÜEDAD			CANTIDAD DE EMPLEADOS		
		Montevideo	Interior	Servicio	Industria	1 a 15 años	16 a 30 años	31 y más	1 a 20	21 a 40	41 y más
Muy adecuadamente	6	11	-----	-----	13	6	-----	17	7	-----	13
Adecuadamente	35	22	54	53	19	50	33	-----	36	33	38
Ni adecuadamente ni inadecuadamente	32	44	15	20	44	25	44	33	36	33	25
Inadecuadamente	19	11	31	27	13	19	11	33	21	33	-----
NS/NC	6	11	-----	-----	13	0	11	17	-----	-----	25

Las empresas que en mayor medida señalan que esta gestión es realizada de manera adecuada son las del interior y aquellas vinculadas a los servicios. Las más críticas serían las más antiguas y aquellas con entre 21 a 40 empleados.

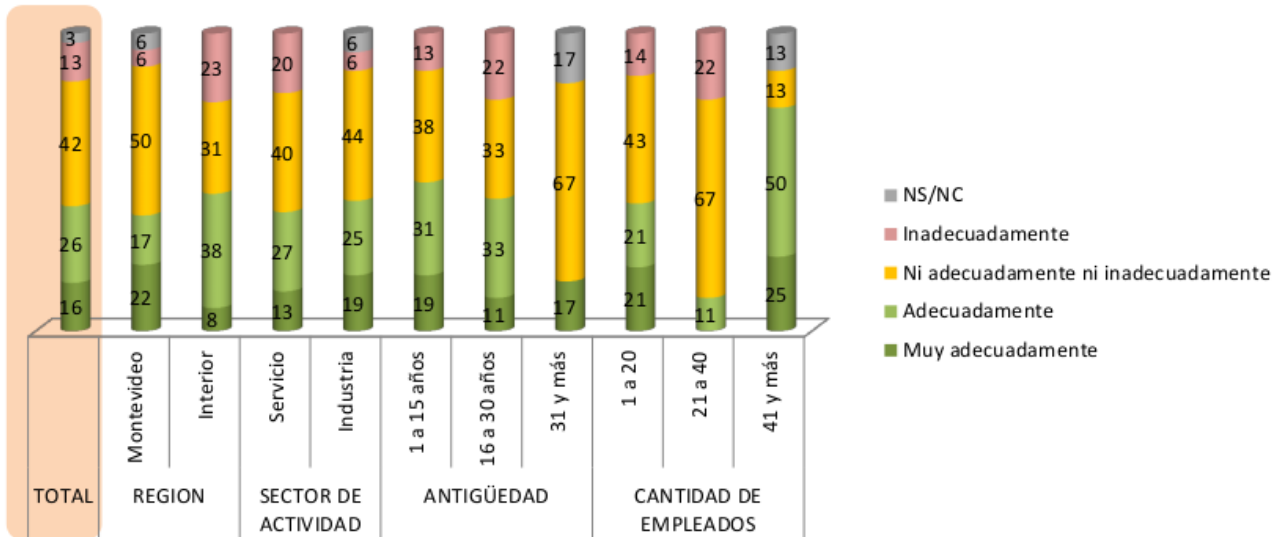
Gráfica 3. RESPUESTA DE RIESGO EN TI.

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P14. A continuación vamos a mencionarle una serie de dimensiones de gobierno, evaluación y respuesta del riesgo en TI, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las gestiona su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).

P14.c. (RESPUESTA DE RIESGO EN TI) Articular el riesgo, gestionar riesgos ocurridos en su empresa y reaccionar a eventos, incidentes de riesgo en TI

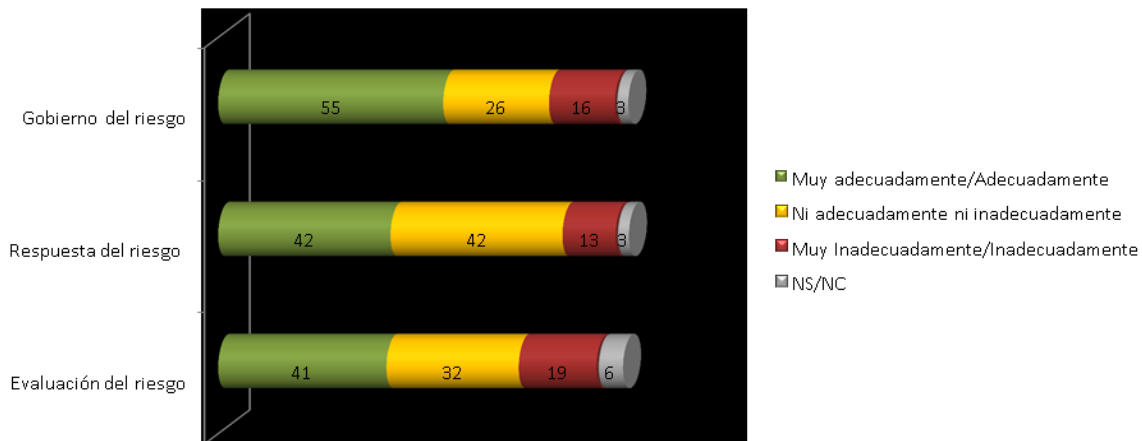


La respuesta al riesgo es un aspecto que las empresas perciben se implementa en escasas situaciones de manera adecuada o muy adecuada. Aquellas empresas que mejor evalúan este ítem son principalmente las que cuentan con mayor cantidad de empleados y las del interior.

Gráfica 4. Gráfico resumen: Dimensiones de gobierno, evaluación y respuesta del riesgo en TI.

N=31 Total de Encuestados

P14. A continuación vamos a mencionarle una serie de dimensiones de gobierno, evaluación y respuesta del riesgo en TI, y le vamos a pedir que califique de 1 a 5 qué tan adecuada o inadecuadamente las gestiona su organización (siendo 1=Muy adecuadamente, 2=Adecuadamente, 3=Ni adecuada ni inadecuadamente, 4=Inadecuadamente y 5=Muy inadecuadamente).



La evaluación de estos ítems no resulta tan favorable como los anteriormente testeado. El atributo mejor evaluado por parte de las empresas sería la gestión del gobierno del riesgo. Por su parte, es la gestión de evaluación de riesgo la que presenta los mayores niveles de percepción de inadecuación.

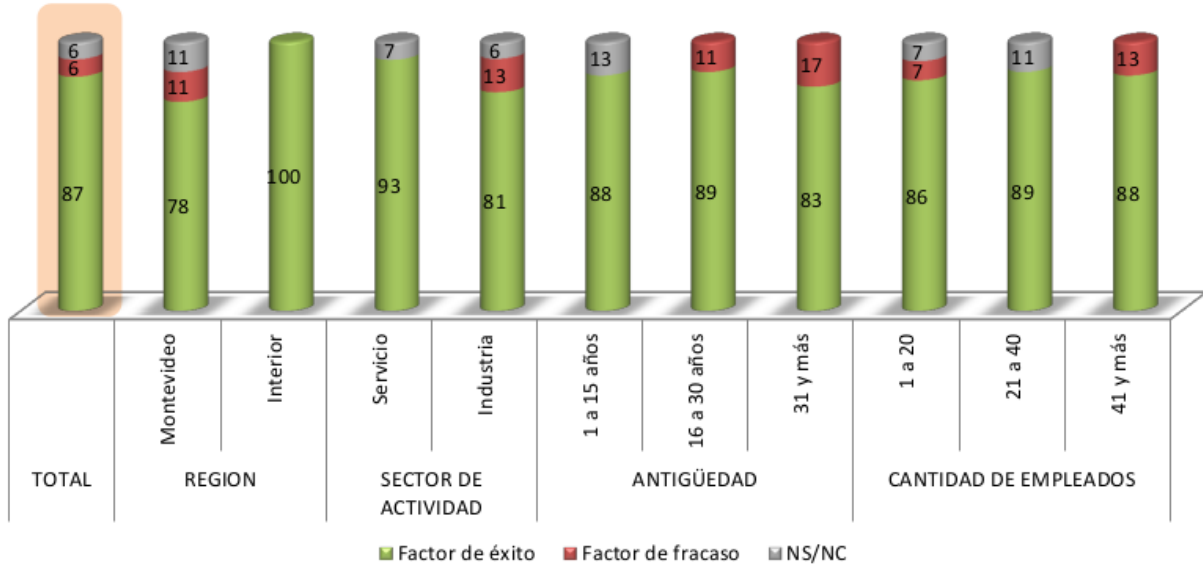
3. Factores de éxito o de obstáculo de la GC en su empresa

Gráfico 1. Factores de éxito y fracaso en la gestión del conocimiento: RECURSOS ECONÓMICOS.

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P15. Finalmente, hay una serie de factores que pueden ser factores de éxito de la GC o bien factores de fracaso u obstáculo de la GC en una organización. Le pedimos nos indique para los siguientes aspectos si son un factor de éxito o de obstáculo para una adecuada implementación de la GC en su organización.



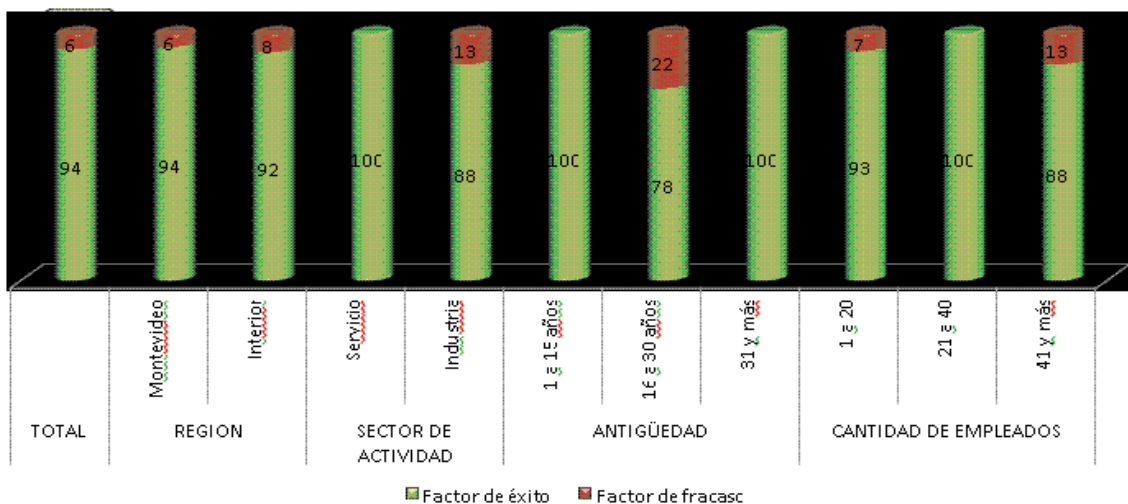
Los recursos económicos son considerados por una abultada mayoría como un factor de éxito para la «gestión del conocimiento». Las PYMES del interior y aquellas orientadas a los servicios, así lo consideran en mayor medida. Las más críticas serían aquellas con mayor antigüedad.

Gráfico 2. Factores de éxito y fracaso en la gestión del conocimiento: RECURSOS HUMANOS

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados

P15. Finalmente, hay una serie de factores que pueden ser factores de éxito de la GC o bien factores de fracaso u obstáculo de la GC en una organización. Le pedimos nos indique para los siguientes aspectos si son un factor de éxito o de obstáculo para una adecuada implementación de la GC en su organización.

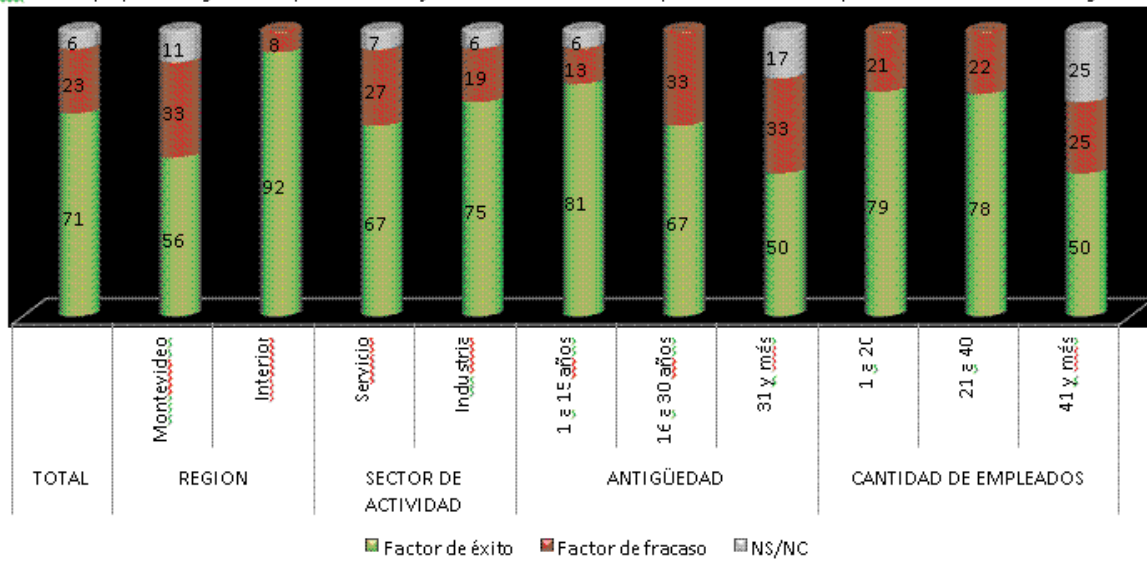


Una amplia mayoría de los encuestados consideran que los recursos humanos son un factor de éxito en esta misma temática. Las PYMES orientadas a la venta de servicios, con menor (y mayor) cantidad de años en ejercicio y de 21 a 40 empleados lo consideran en mayor medida. Las diferencias entre en resto de las categorías no se presentan como estadísticamente significativas.

Gráfico 3. Factores de éxito y fracaso en la gestión del conocimiento: RECURSOS DE TIEMPO

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P15. Finalmente, hay una serie de factores que pueden ser factores de éxito de la GC o bien factores de fracaso u obstáculo de la GC en una organización. Le pedimos nos indique para los siguientes aspectos si son un factor de éxito o de obstáculo para una adecuada implementación de la GC en su organización.



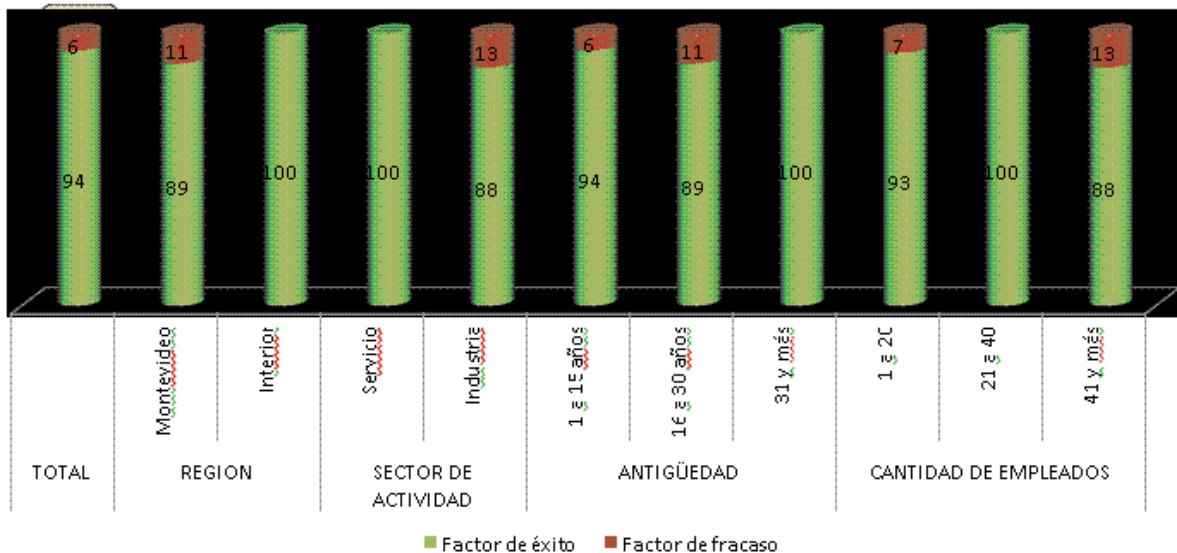
Una amplia mayoría de los encuestados considera que los recursos de tiempo son un factor de éxito dentro de su empresa. Principalmente se destaca esta percepción entre las PYMES del interior, del sector de industria con menos años de antigüedad en el mercado y menos de 41 empleados.

Gráfico 4. Factores de éxito y fracaso en la gestión del conocimiento: COMPROMISO DE LA DIRECCIÓN

N=31 Total de encuestados.

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P15. Finalmente, hay una serie de factores que pueden ser factores de éxito de la GC o bien factores de fracaso u obstáculo de la GC en una organización. Le pedimos nos indique para los siguientes aspectos si son un factor de éxito o de obstáculo para una adecuada implementación de la GC en su organización.

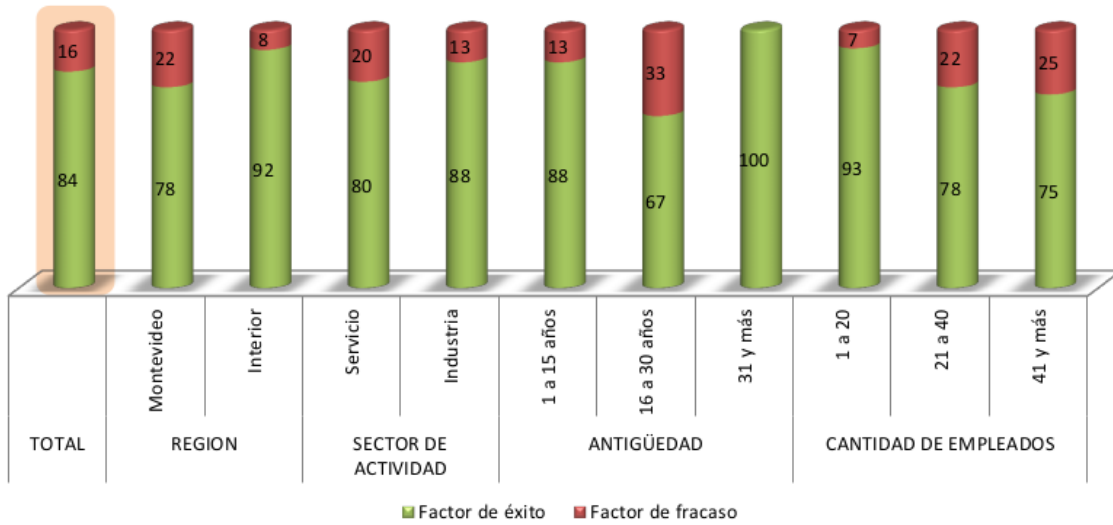


Una gran mayoría de 94% se destaca que el «compromiso de la dirección», es un factor de éxito para la Gestión del Conocimiento dentro de la empresa. Esto se destaca principalmente en el interior y en las empresas dedicadas al sector servicios, así como también aquellas con menor cantidad de empleados (menos de 40 empleados) y más antigüedad.

Gráfico 5. Factores de éxito y fracaso en la gestión del conocimiento: CULTURA ORGANIZACIONAL
 Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

N=31 Total de Encuestados

P15. Finalmente, hay una serie de factores que pueden ser factores de éxito de la GC o bien factores de fracaso u obstáculo de la GC en una organización. Le pedimos nos indique para los siguientes aspectos si son un factor de éxito o de obstáculo para una adecuada implementación de la GC en su organización.

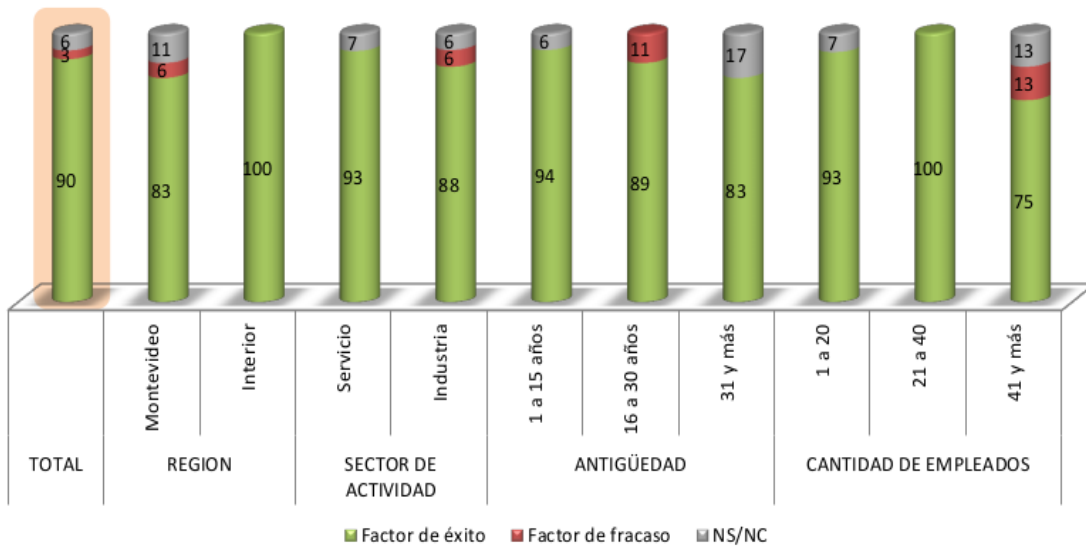


Un 84% de los encuestados consideran a la cultura organizacional como un factor de éxito. En el interior, las empresas de mayor cantidad de años y menor cantidad de empleados lo consideran así en mayor medida.

Gráfico 6. Factores de éxito y fracaso en la gestión del conocimiento: MARCOS DISPONIBLES DE BUENAS PRÁCTICAS
 Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

N=31 Total de Encuestados

P15. Finalmente, hay una serie de factores que pueden ser factores de éxito de la GC o bien factores de fracaso u obstáculo de la GC en una organización. Le pedimos nos indique para los siguientes aspectos si son un factor de éxito o de obstáculo para una adecuada implementación de la GC en su organización.



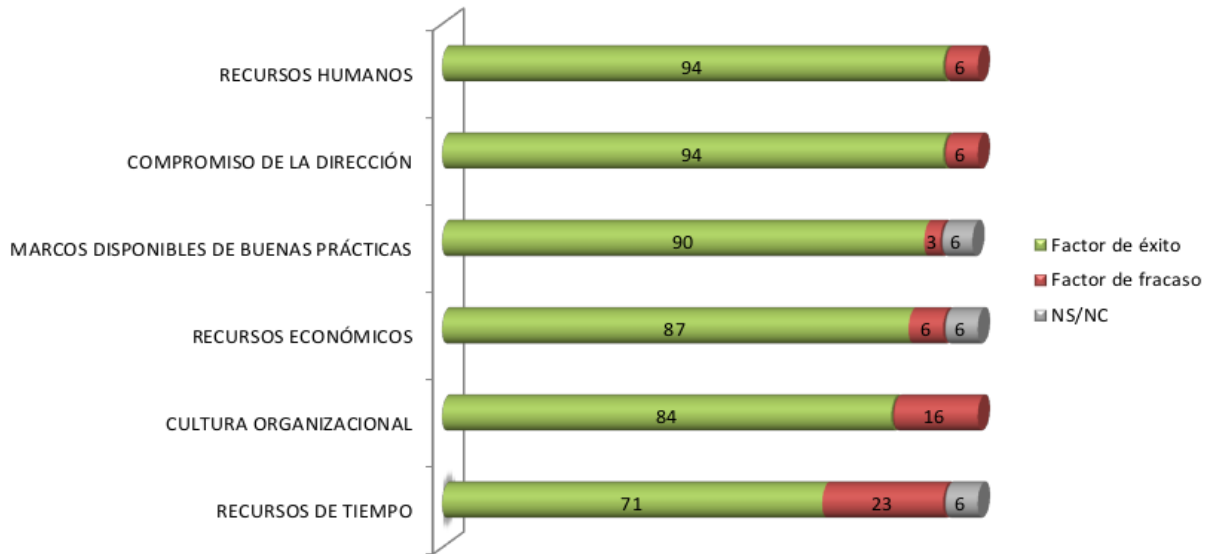
Una amplia mayoría encuentra como factor de éxito los marcos disponibles de buenas prácticas. En el interior, las empresas de menor cantidad de años de ejercicio y de 21 a 40 empleados encuentran en este aspecto un factor muy relevante de éxito de la Gestión del Conocimiento en su organización.

Gráfico 7. Factores de éxito y fracaso en la gestión del conocimiento: RESUMEN

N=31 Total de Encuestados

Segmentos: región, sector de actividad, antigüedad y cantidad de empleados.

P15. Finalmente, hay una serie de factores que pueden ser factores de éxito de la GC o bien factores de fracaso u obstáculo de la GC en una organización. Le pedimos nos indique para los siguientes aspectos si son un factor de éxito o de obstáculo para una adecuada implementación de la GC en su organización.



De acuerdo con el gráfico resumen en general todos los ítems mencionados se consideran en mayor medida como factores de éxito de la Gestión del Conocimiento en sus empresas. Sin embargo, los factores que son en menor proporción percibido como los de éxito serían «los recursos de tiempo», «la cultura organizacional» y «los recursos económicos».

4. Conclusiones

Caracterización de la muestra.

La muestra está compuesta mayoritariamente por empresas de Montevideo 58%. En relación al sector de actividad, 48% de las PYMES se dedican al sector servicios y un 52% al sector industrial. En su mayoría son empresas jóvenes, de 1 a 15 años de funcionamiento, y considerando la cantidad de empleados son en su mayoría pequeñas empresas.

La Gestión del Conocimiento en la estrategia de la empresa

-La gestión de conocimiento en su mayoría se considera un aspecto importante y muy importante para la consecución de la estrategia, misión y visión de la empresa. Las principales razones, que exponen los encuestados para considerarlo importante es porque se considera que posibilita alcanzar resultados, aumentar conocimientos, satisfacer al cliente y capacitar empleados.

-Un 42% de los encuestados sostiene que en su organización existe una estrategia implementada y sistematizada en relación a la gestión del conocimiento.

-Es importante tener en cuenta que a mayor antigüedad, existe una mayor probabilidad de encontrarse con PYMES en la que sus trabajadores dicen que se desarrollan actividades relacionadas a la gestión del conocimiento pero de forma aislada, sin estrategia o que directamente declaran que no existen actividades en dirección o con perspectiva de gestión del conocimiento.

-Son los gerentes quienes en mayor medida participan en la definición e implementación de la estrategia de gestión del conocimiento.

Etapas de la Gestión del Conocimiento realizadas en la empresa

-En lo que respecta a las fases del ciclo de gestión del conocimiento, se registran valores muy adecuados. Resaltándose mayores dificultades en la retención, la identificación y la adquisición del conocimiento.

Herramientas y técnicas de la GC utilizadas en la empresa

-En relación a la aplicación de herramientas y técnicas de gestión del conocimiento evaluadas, se registran niveles de adecuación. Aunque se encuentran dificultades en la herramienta de grupos expertos y círculos de calidad, así como también en lecciones aprendidas y clasificación y clustering.

Dimensiones de gobierno, evaluación y respuesta del riesgo en TI

-La Gestión de la evaluación del riesgo junto con respuesta ante el riesgo, parecen ser los aspectos en los que se demuestran mayores dificultades.

Factores de éxito o de obstáculo de la GC en su empresa

A pesar de que todos los factores resultan mayoritariamente considerados como de éxito, corresponde destacar que son los RRHH y el compromiso por parte de la dirección los que en mayor medida son visualizados como de éxito. Por otra parte, los que cuentan con mayor porcentaje de consideraciones como factores de fracaso u obstáculo son los recursos referentes al tiempo y a la cultura organizacional.

ANEXO VI - Estudio de la incidencia de la cantidad de empleados – cantidad de empleados de TI

ÍNDICE DE INFORME

0 Ficha metodológica	2
1. La Empresa	4
2. Alineamiento de TI con la estrategia de la Empresa	24
3. Aportación de valor	32
4 Seguridad	38
5 Internet	51
6 Toma de decisiones	67
7 Gobierno de las TI	74
8 Conocimiento de herramientas y organizaciones gobernanza de TI	104

0. FICHA METODOLÓGICA

Tipo de estudio

- Entrevistas Cara a Cara.
- 30 casos a Directores Generales, Directores Financieros, Directores de Departamento y Directores de TI de pequeñas y medianas empresas (hasta 100 trabajadores).
- Duración de las entrevistas: 45 minutos

Confección de la muestra

- **Muestra:** Muestra No Probabilística de Criterio/Intencional. El criterio de selección que prima es el criterio personal del investigador acerca de la representatividad y heterogeneidad de la población que se está estudiando. Por ello la selección incluyó una distribución heterogénea de rubros, tipos de empresas (industriales y de servicios), y zonas del país (departamentos de Montevideo, Maldonado, San José y Colonia).
- **Margen de Error:** No se puede calcular el error muestral por tratarse de una muestra no probabilística.
- **Sujeto Encuestado:** Directores Generales, Directores Financieros, Directores de Departamento y Directores de TI de las empresas
- **Unidad de Análisis:** PYMES (pequeñas y medianas empresas).
- **Universo:** PYMES (pequeñas y medianas empresas).

Procesamiento de la información

Las encuestas son codificadas e ingresadas a una base de datos que se depura controlando inconsistencias. La información se procesa mediante programa informático estadístico SPSS.

Alcance del Estudio

El informe presentado corresponde a los resultados de la aplicación de la encuesta durante los meses de julio – agosto de 2010.

Resultados de Campo:

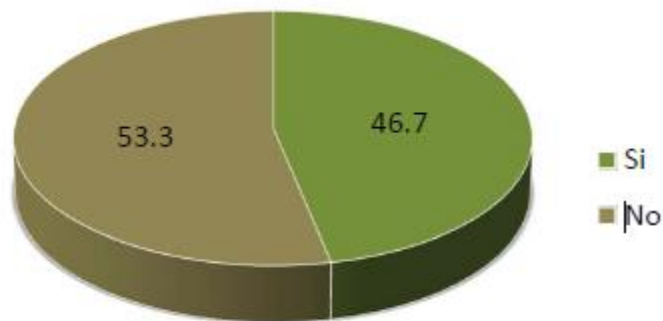
Del total de contactos efectuados, 100% constituyeron entrevistas efectivas, no existiendo ningún rechazo.

1. LA EMPRESA

1.1.1 Dimensión y estructura de TI en la empresa

¿Existe una estructura de TI definida en la empresa?

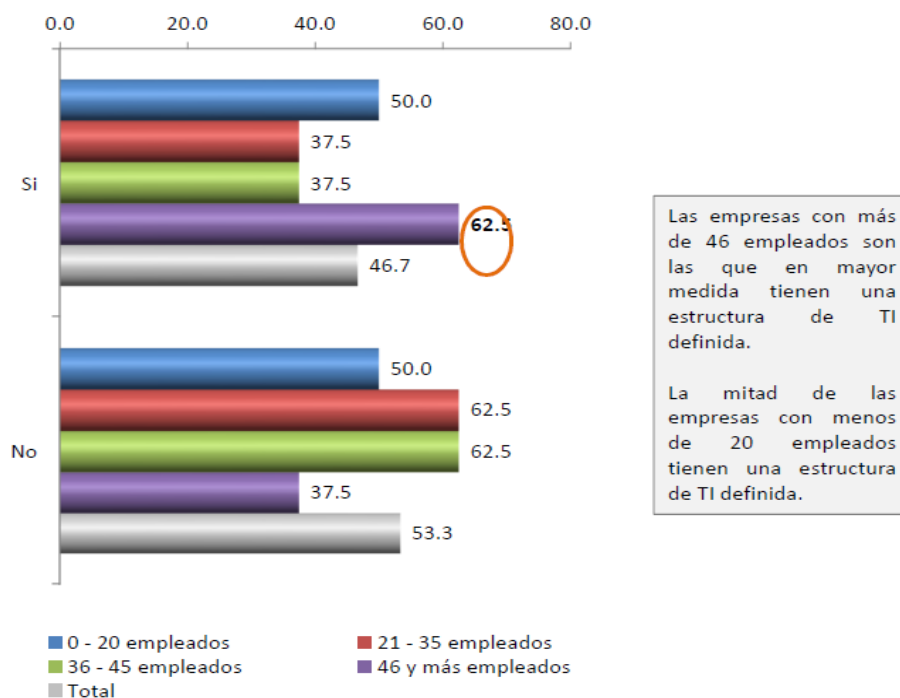
Gráfica 1. Existencia de una estructura definida de TI



El 46,7% de las empresas tiene una estructura definida de TI, mientras que el 53,3 % no la tiene.

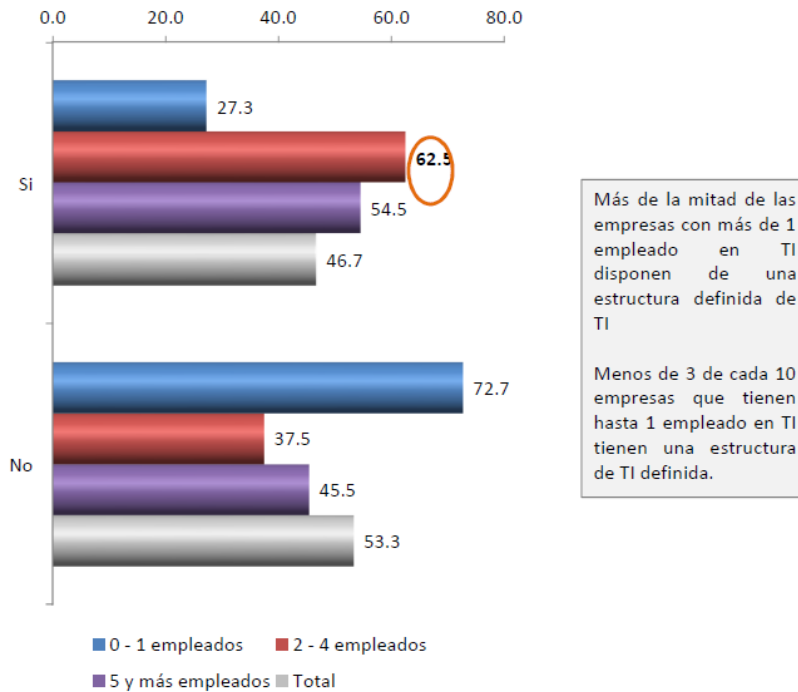
1.2.1 Dimensión y estructura de TI en la empresa según Cantidad de Empleados

Gráfica 2. ¿Existe una estructura de TI definida en la empresa?



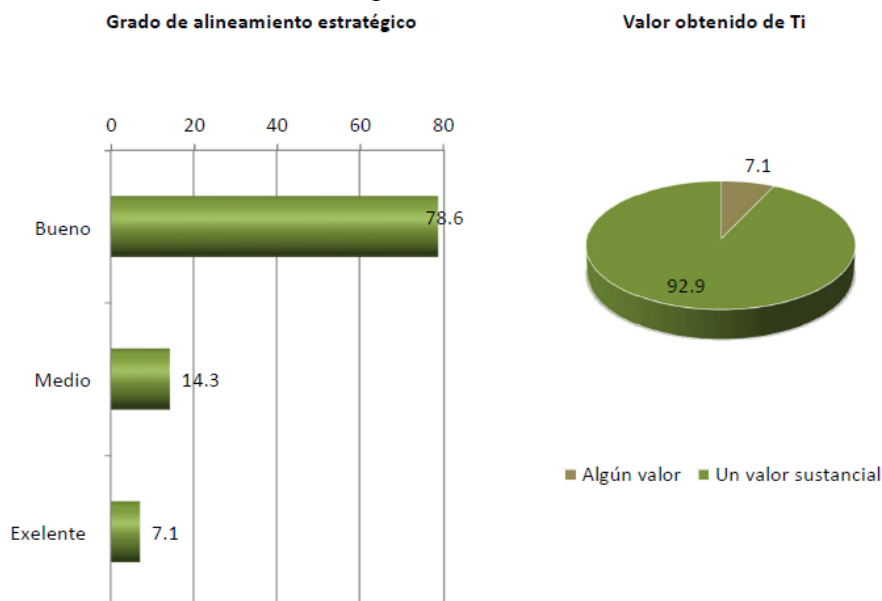
1.3.1 Dimensión y estructura de TI en la empresa Cantidad de Empleados TI

Grafica 3. ¿Existe una estructura de TI definida en la empresa?



1.4.1.1 Empresas con infraestructura de TI en relación al grado de alineamiento estratégico y la entrega de valor de TI

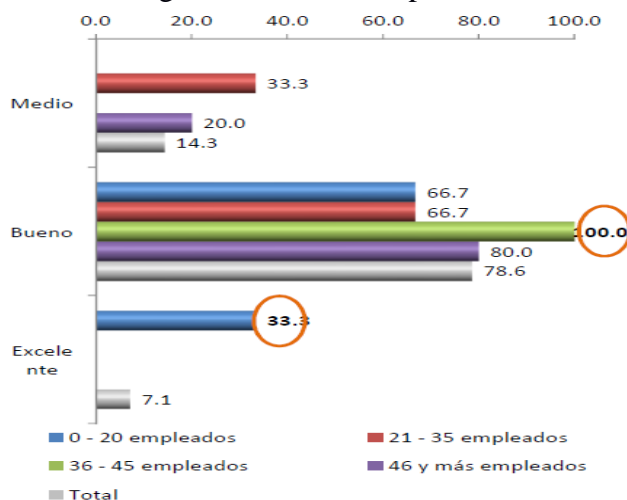
Grafica 4. Empresas con infraestructura de TI en relación al grado de alineamiento estratégico y la entrega de valor de TI



Analizando las empresas que tienen una infraestructura de TI en relación al grado de alineamiento estratégico, puede verse que el 78% lo evalúa como bueno y el 14% entiende que es medio. Si se analiza las empresas que cuentan con infraestructura según el valor obtenido de TI, se observa que el 92% considera que está obteniendo un valor sustancial de TI y el 7% expresa que obtiene algún valor de TI en su organización.

1.4.1.2 Empresas con infraestructura de TI en relación al grado de alineamiento estratégico según Cantidad de Empleados

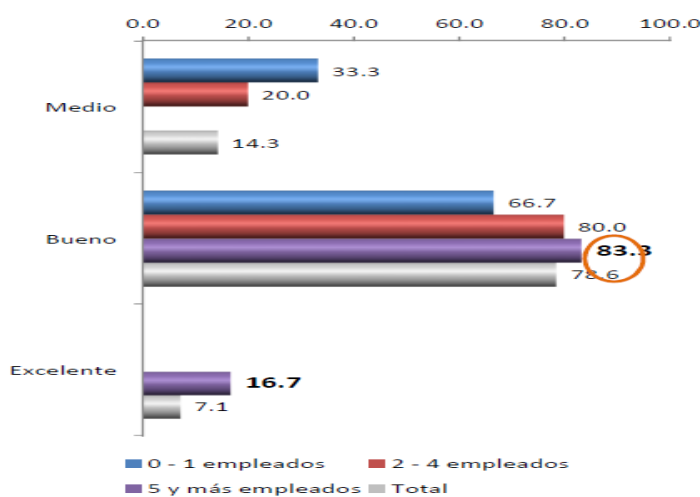
Grafica 5. Empresas con infraestructura de TI en relación al grado de alineamiento estratégico según cantidad de empleados



Quienes evalúan en mayor medida como «bueno» el grado de alineamiento estratégico son las empresas que tienen entre 36 y 45 empleados. Las empresas con menos de 20 empleados son las únicas que evalúan el grado de alineamiento como excelente.

1.4.1.3 Empresas con infraestructura de TI en relación al grado de alineamiento estratégico según Cantidad de Empleados TI

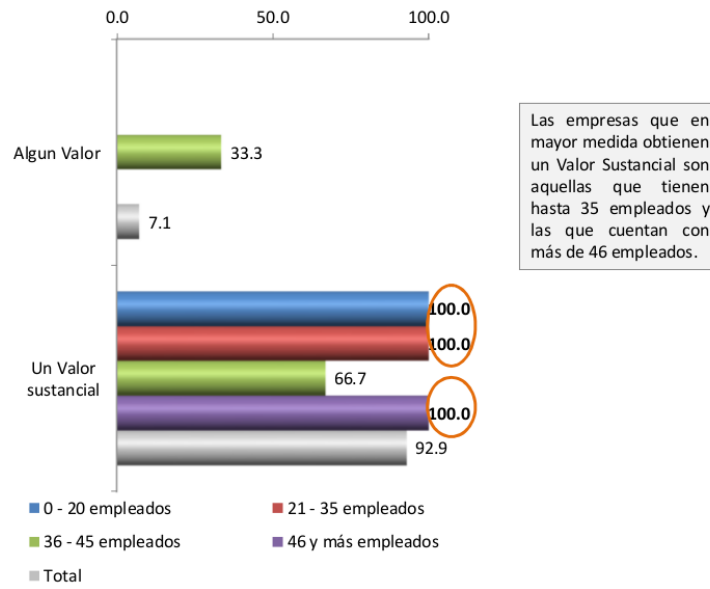
Grafica 6. Empresas con infraestructura de TI en relación al grado de alineamiento estratégico según cantidad de empleados TI



A medida que aumenta la cantidad de empleados de TI mejora la evaluación del alineamiento estratégico entre la estrategia o visión global de TI y la estrategia o visión global de la organización.

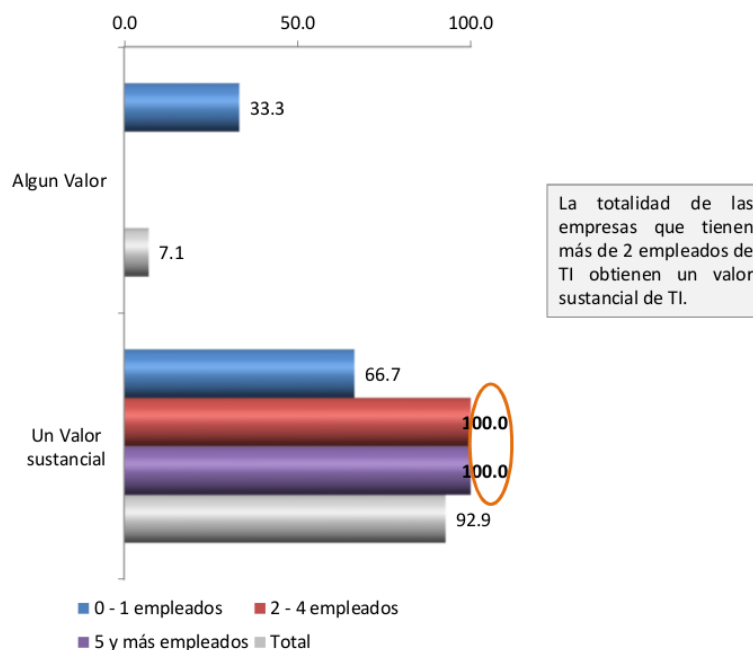
1.4.1.4 Empresas con infraestructura de TI en relación a la entrega de valor de TI según Cantidad de Empleados

Grafica 7. Empresas con infraestructura de TI en relación a la entrega de valor de TI según cantidad de empleados



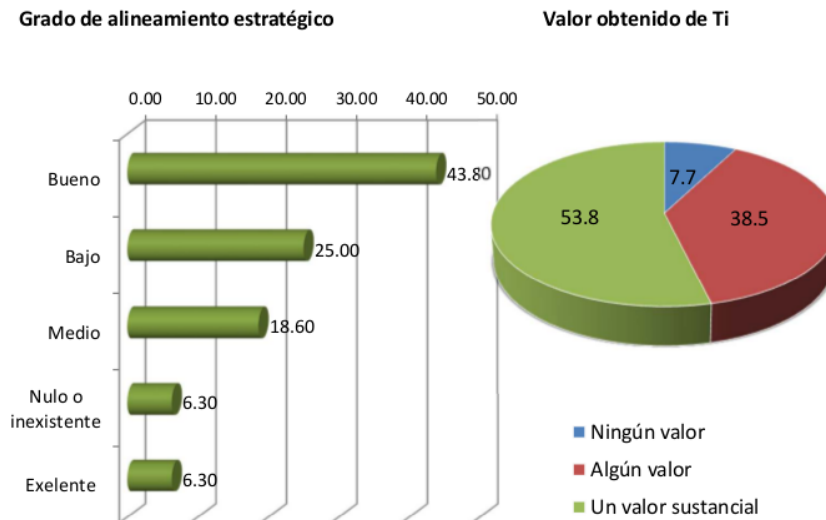
1.4.1.5 Empresas con infraestructura de TI en relación a la entrega de valor de TI según Cantidad de Empleados TI

Grafica 8. Empresas con infraestructura de TI en relación a la entrega de valor de TI según cantidad de empleados TI



1.4.2.1 Empresas que no cuentan con infraestructura de TI en relación al grado de alineamiento estratégico y la entrega de valor de TI

Grafica 9. Empresas que no cuentan con infraestructura de TI en relación al grado de alineamiento estratégico y la entrega de valor de TI

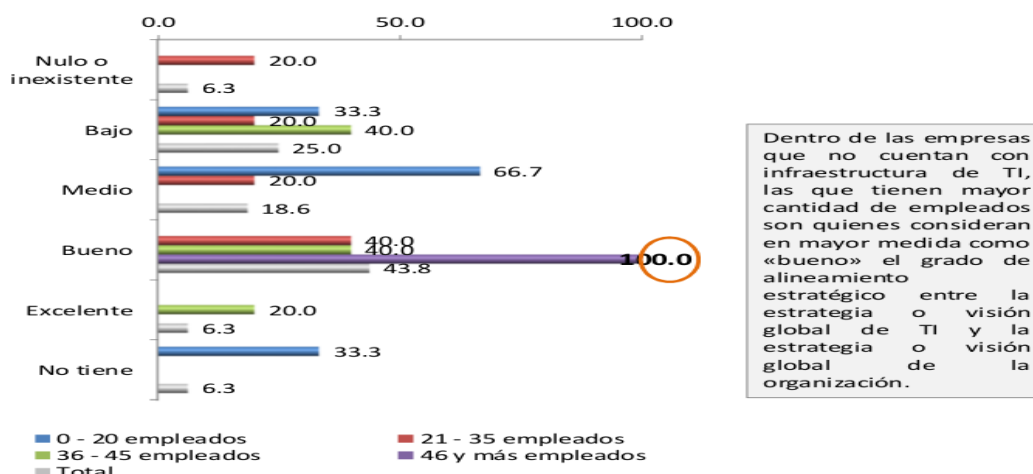


Analizando las empresas que no tienen una infraestructura de TI en relación al grado de alineamiento estratégico, puede verse que el 43% lo evalúa como bueno y el 25% entiende que es bajo.

Si se analiza las empresas que cuentan con infraestructura según el valor obtenido de TI, se observa que el 54% considera que está obteniendo un valor sustancial de TI, el 38% expresa que obtiene algún valor de TI en su organización y el restante 7% entiende que no obtiene ningún valor de TI.

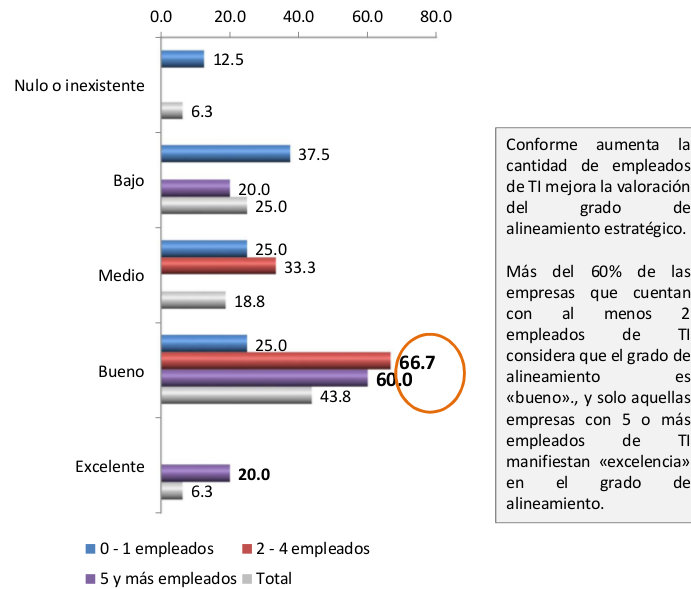
1.4.2.2 Empresas que no cuentan con infraestructura de TI en relación al grado de alineamiento estratégico según Cantidad de Empleados

Grafica 10. Empresas que no cuentan con infraestructura de TI en relación al grado de alineamiento estratégico según cantidad de empleados



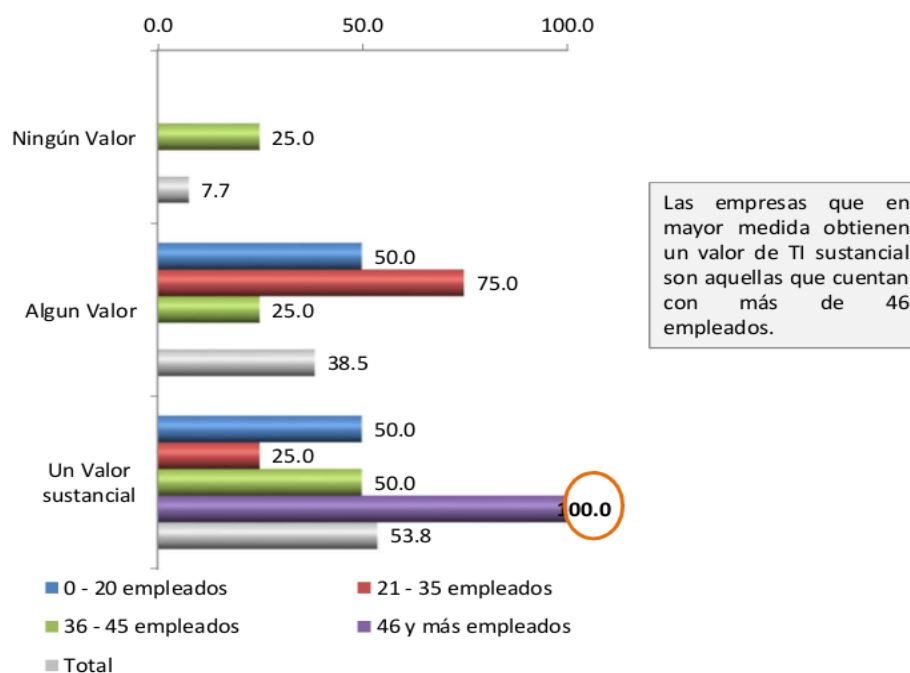
1.4.2.3 Empresas que no cuentan con infraestructura de TI en relación al grado de alineamiento estratégico según Cantidad de Empleados de TI

Grafica 11. Empresas que no cuentan con infraestructura de TI en relación al grado de alineamiento estratégico según cantidad de empleados de TI



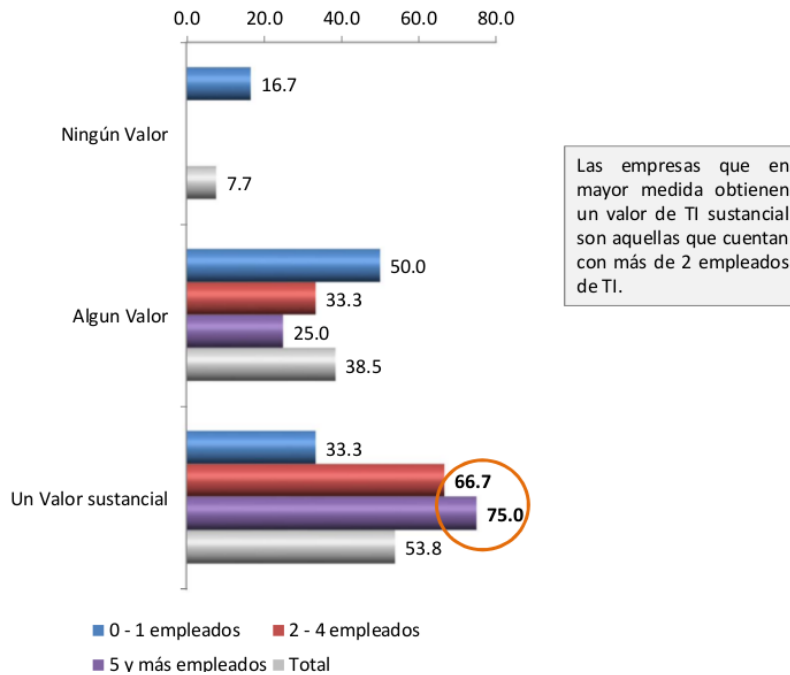
1.4.2.4 Empresas que no cuentan con infraestructura de TI en relación a la entrega de valor de TI según Cantidad de Empleados

Grafica 12. Empresas que no cuentan con infraestructura de TI en relación a la entrega de valor de TI según cantidad de empleados



1.4.2.5 Empresas que no cuentan con infraestructura de TI en relación a la entrega de valor de TI según Cantidad de Empleados de TI

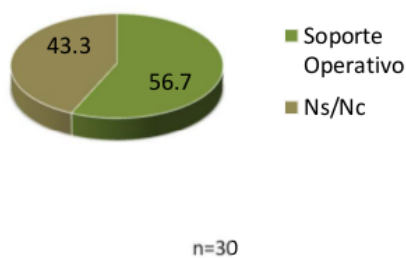
Grafica 13. Empresas que no cuentan con infraestructura de TI en relación a la entrega de valor de TI según cantidad de empleados de TI



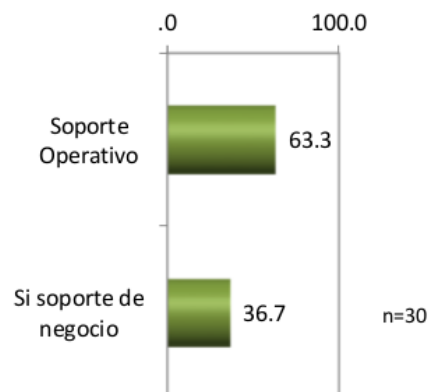
1.4.3 Dimensión y estructura de TI en la empresa

Grafica 14. Responsabilidad de TI y soporte al negocio

Gráfica 9. Responsabilidad de TI



Gráfica 10. Soporte al negocio



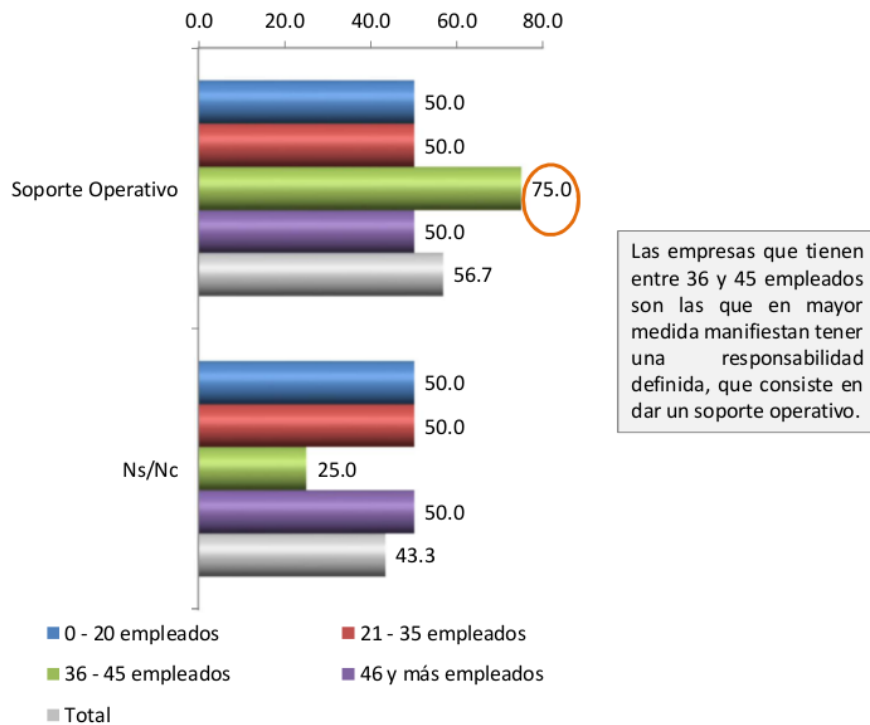
Respecto a la responsabilidad de TI, solo un 56,7% respondió tener una responsabilidad definida, que consiste en dar un soporte operativo.

En el gráfico 10, se muestra, el soporte al negocio. Puede verse que el 36,7% tiene un soporte de negocio.

El 63,3% de las empresas expreso que solo tiene un soporte operativo.

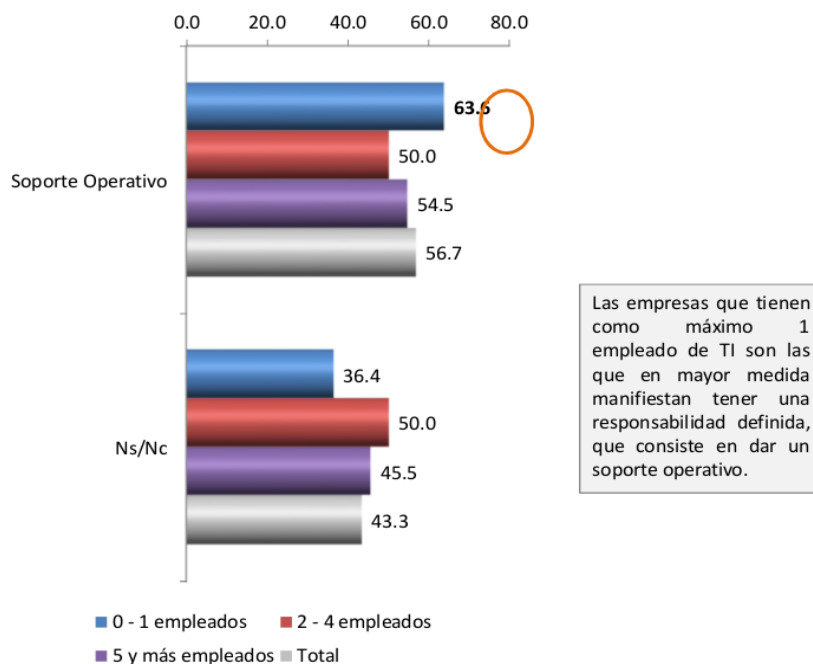
1.4.4 Dimensión y estructura de TI en la empresa

Grafica 15. Responsabilidad de TI según Cantidad de Empleados



1.4.5 Dimensión y estructura de TI en la empresa

Grafica 16. Responsabilidad de TI según Cantidad de Empleados de TI



1.4.6 Dimensión y estructura de TI en la empresa

% de presupuesto	% de casos
50	7,7
40	7,7
30	7,7
25	7,7
15	7,7
10	23,1
8	7,7
5	23,1
3	7,7

Figura 1. Presupuesto asignado a TI

El presupuesto asignado de las empresas a TI, en promedio es de 16,58%.

El 23,1% de las empresas asignan un 5% y un 10% de su presupuesto a TI.

Como se ve en la tabla, los presupuestos asignados a TI van desde un 3% hasta un 50%.

1.4.7 Dimensión y estructura de TI en la empresa

	21 - 35 empleados	36 - 45 empleados	46 y más empleados	Total
3%	0,0	25,0	0,0	7,7
5%	20,0	25,0	25,0	23,1
8%	20,0	0,0	0,0	7,7
10%	40,0	25,0	0,0	23,1
15%	0,0	0,0	25,0	7,7
25%	0,0	25,0	0,0	7,7
30%	0,0	0,0	25,0	7,7
40%	20,0	0,0	0,0	7,7
50%	0,0	0,0	25,0	7,7

3 de cada 4 empresas (75%) que tienen más de 46 empleados asignan más del 15% de su presupuesto a TI. En cambio, las empresas con menos de 45 empleados que asignan más del 15% del presupuesto a TI solo representan algo más del 20%.

Figura 2. Presupuesto asignado a TI según Cantidad de Empleados

1.4.8 Dimensión y estructura de TI en la empresa

	0 - 1 empleados	2 - 4 empleados	5 y más empleados	Total
3%	0,0	20,0	0,0	7,7
5%	50,0	20,0	16,7	23,1
8%	0,0	20,0	0,0	7,7
10%	50,0	0,0	33,3	23,1
15%	0,0	20,0	0,0	7,7
25%	0,0	0,0	16,7	7,7
30%	0,0	20,0	0,0	7,7
40%	0,0	0,0	16,7	7,7
50%	0,0	0,0	16,7	7,7

1 de cada 3 empresas que tiene más de 5 empleados de TI asigna más del 40% de su presupuesto a TI.
 Las empresas con 0 o 1 empleado de TI asignan como máximo un 10 de su presupuesto.
 Un 20% de las empresas con 2 a 4 empleados de TI asignan el 30% de su presupuesto a TI.

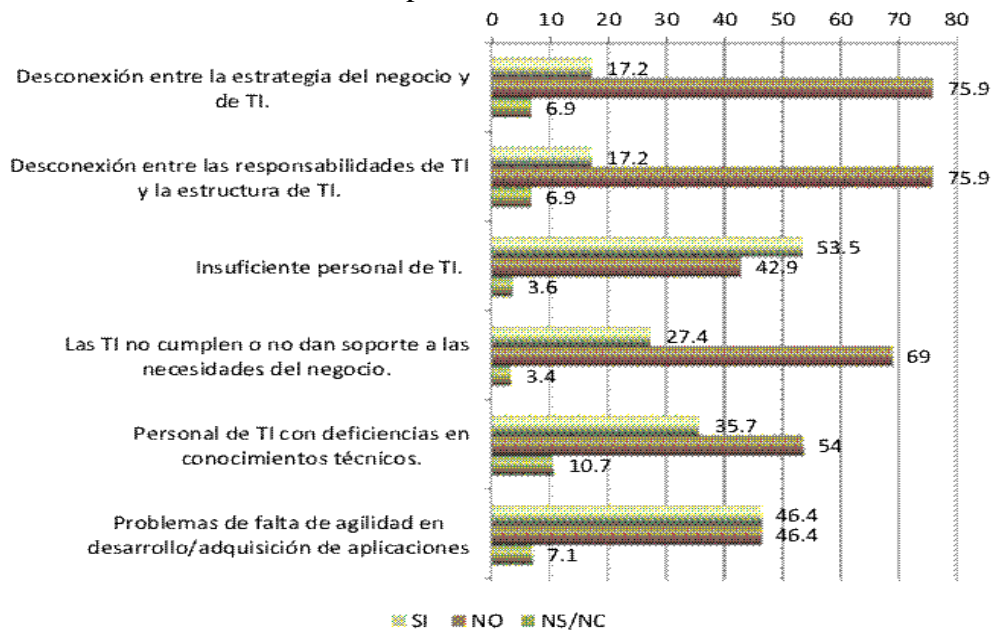
Figura 3. Presupuesto asignado a TI según Cantidad de Empleados de TI

2. ALINEAMIENTO DE TI CON LA ESTRATEGIA DE LA EMPRESA

2.1 Problemas experimentados en las TI los últimos 12 meses

¿Cuál de los siguientes problemas ha experimentado en las TI los últimos 12 meses?

Grafica 17. Problemas experimentados en las TI los últimos 12 meses



El problema más frecuente que se ha experimentado en los últimos 12 meses, con un 60,7% de las empresas entrevistadas es la inexistencia de indicadores de eficiencia de TI. El segundo problema más frecuente es la inexistencia de procesos de revisión y evaluación de los indicadores y objetivos de TI.

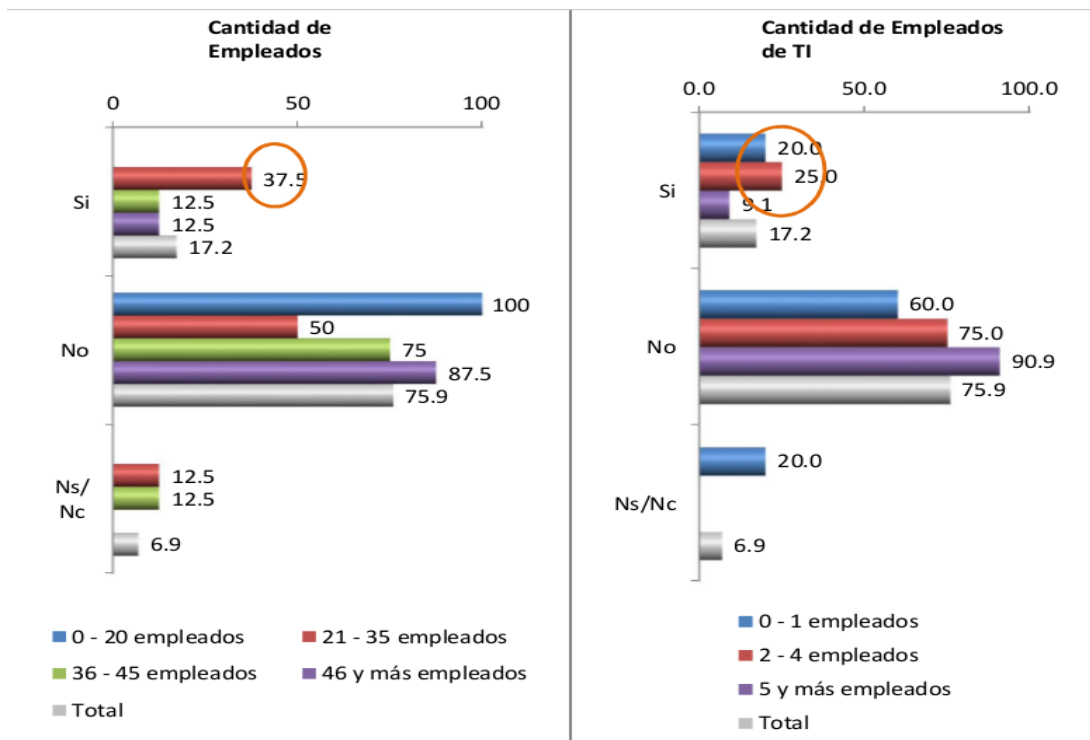
Para un 53,5% de los entrevistados, los problemas experimentados tienen que ver con la insuficiencia de personal de TI.

En cuarto lugar, el problema refiere a la inexistencia de un plan de Continuidad del Negocio.

Finalmente en último lugar se encuentran problemas relacionados con la inexistencia de indicadores de calidad de servicios Ti y problemas por falta de agilidad de desarrollo/adquisición de aplicaciones.

2.2 Problemas experimentados en las TI los últimos 12 meses: Desconexión entre la estrategia del negocio y de TI según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 18. Problemas experimentados en las TI los últimos 12 meses: Desconexión entre la estrategia del negocio y de TI según cantidad de empleados y cantidad de empleados de TI

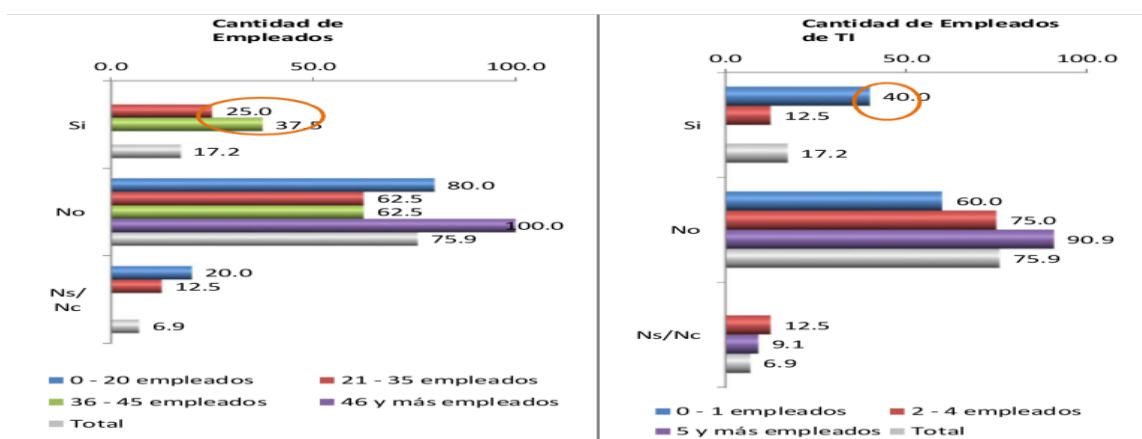


Cantidad de Empleados - Las empresas que tienen entre 21 y 35 empleados son las que manifiestan en mayor medida haber experimentado una desconexión entre la estrategia del negocio y de TI en los últimos 12 meses.

Cantidad de Empleados de TI - Quienes manifiestan en mayor medida haber sufrido dicha desconexión son las empresas con menos de 5 empleados de TI.

2.3 Problemas experimentados en las TI los últimos 12 meses: Desconexión entre las responsabilidades de TI y la estructura de TI según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 19. Problemas experimentados en las TI los últimos 12 meses: Desconexión entre las responsabilidades de TI y la estructura de TI según Cantidad de Empleados y Cantidad de Empleados de TI



Cantidad de Empleados - Solo las **Cantidad de Empleados de TI** – empresas que tienen entre 21 y 45 Quienes manifiestan en mayor medida empleados son las que manifiestan haber sufrido dicha desconexión son las experimentado una desconexión entre las empresas con menos de 2 empleados de responsabilidades de TI y la estructura de TI.
TI.

FICHA METODOLÓGICA

Tipo de estudio

- Entrevistas Cara a Cara.
- 30 casos a Directores Generales, Directores Financieros, Directores de Departamento y Directores de TI de pequeñas y medianas empresas (hasta 100 trabajadores).
- Duración de las entrevistas: 45 minutos

Confección de la muestra

- **Muestra:** Muestra No Probabilística de Criterio/Intencional. El criterio de selección que prima es el criterio personal del investigador acerca de la representatividad y heterogeneidad de la población que se está estudiando. Por ello la selección incluyó una distribución heterogénea de rubros, tipos de empresas (industriales y de servicios), y zonas del país (departamentos de Montevideo, Maldonado, San José y Colonia).
- **Margen de Error:** No se puede calcular el error muestral por tratarse de una muestra no probabilística.
- **Sujeto Encuestado:** Directores Generales, Directores Financieros, Directores de Departamento y Directores de TI de las empresas
- **Unidad de Análisis:** PYMES (pequeñas y medianas empresas).
- **Universo:** PYMES (pequeñas y medianas empresas).

Procesamiento de la información

Las encuestas son codificadas e ingresadas a una base de datos que se depura controlando inconsistencias. La información se procesa mediante programa informático estadístico SPSS.

Alcance del Estudio

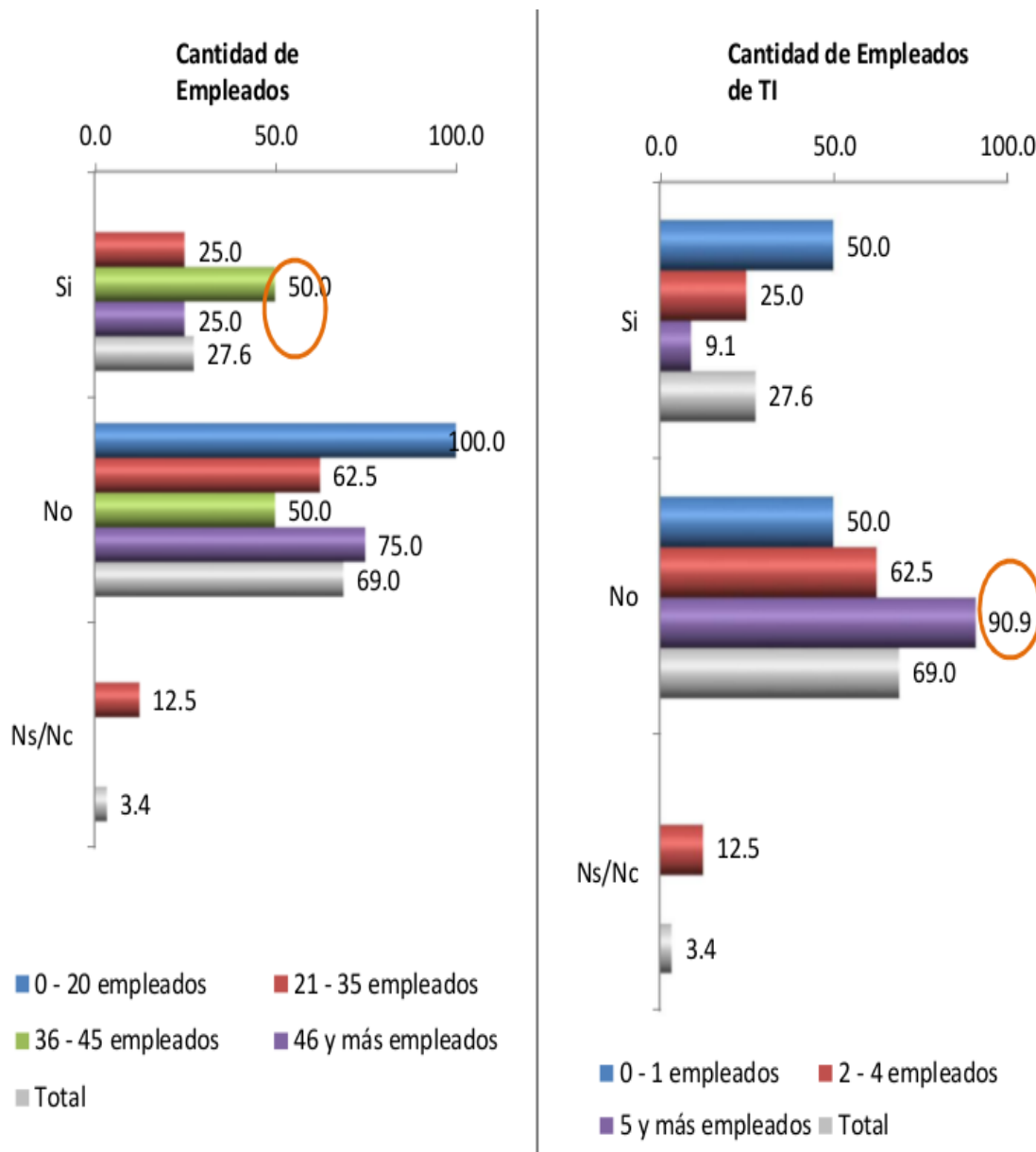
El informe presentado corresponde a los resultados de la aplicación de la encuesta durante los meses de julio – agosto de 2010.

Resultados de Campo:

Del total de contactos efectuados, 100% constituyeron entrevistas efectivas, no existiendo ningún rechazo.

2.4 Problemas experimentados en las TI los últimos 12 meses: Las TI no cumplen o no dan soporte a las necesidades del negocio según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 20. Problemas experimentados en las TI los últimos 12 meses: Las TI no cumplen o no dan soporte a las necesidades del negocio según Cantidad de Empleados y Cantidad de Empleados de TI

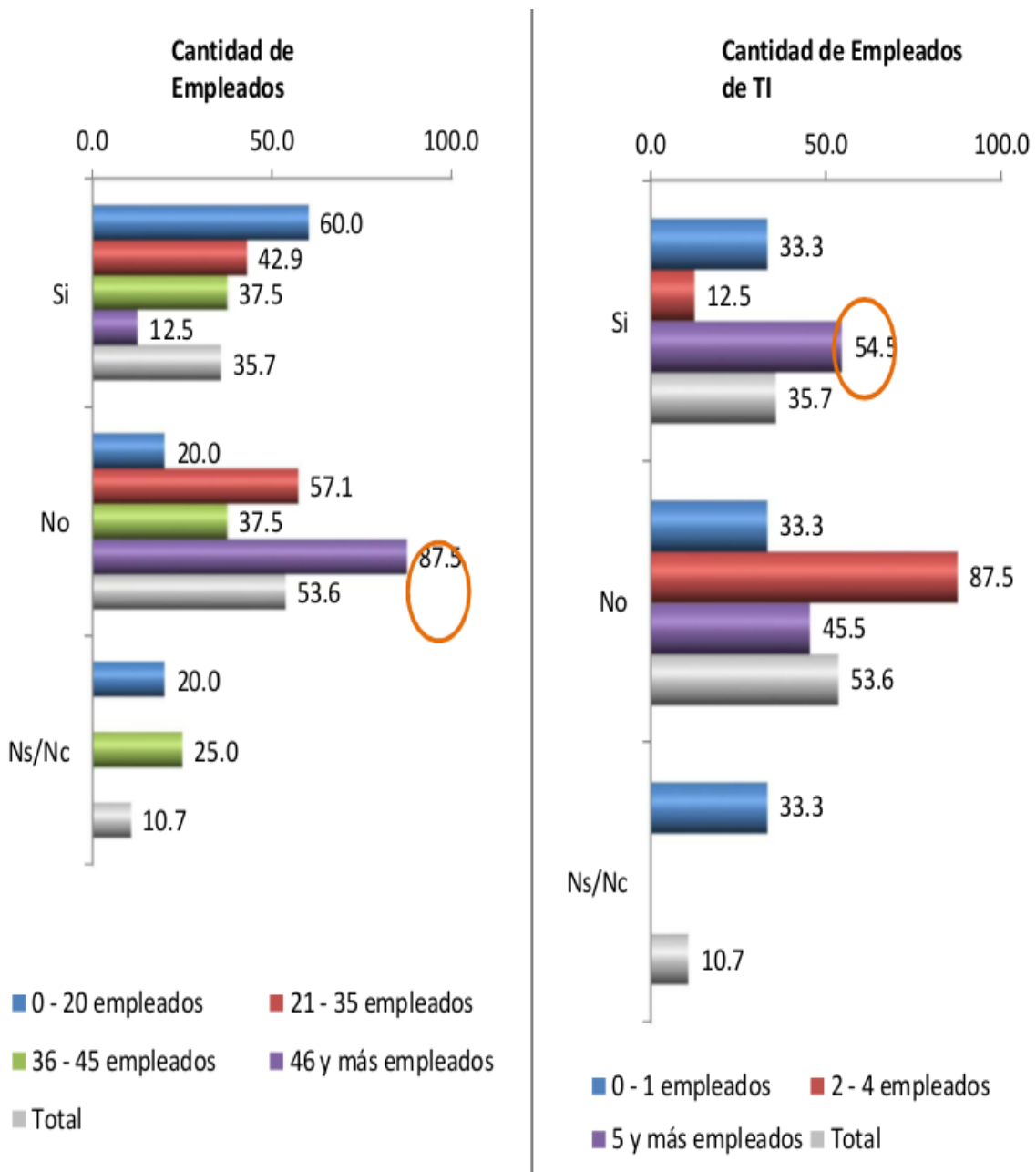


Cantidad de Empleados - Son las empresas que tienen entre 36 y 45 empleados las que manifiestan en mayor medida que las TI no cumplen o no dan soporte a las necesidades del negocio.

Cantidad de Empleados de TI - Conforme aumenta la cantidad de empleados de TI disminuye la existencia de este problema en los últimos 12 meses.

2.5 Problemas experimentados en las TI los últimos 12 meses: Personal de TI con deficiencias en conocimientos técnicos según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 21. Problemas experimentados en las TI los últimos 12 meses: Personal de TI con deficiencias en conocimientos técnicos según Cantidad de Empleados y Cantidad de Empleados de TI

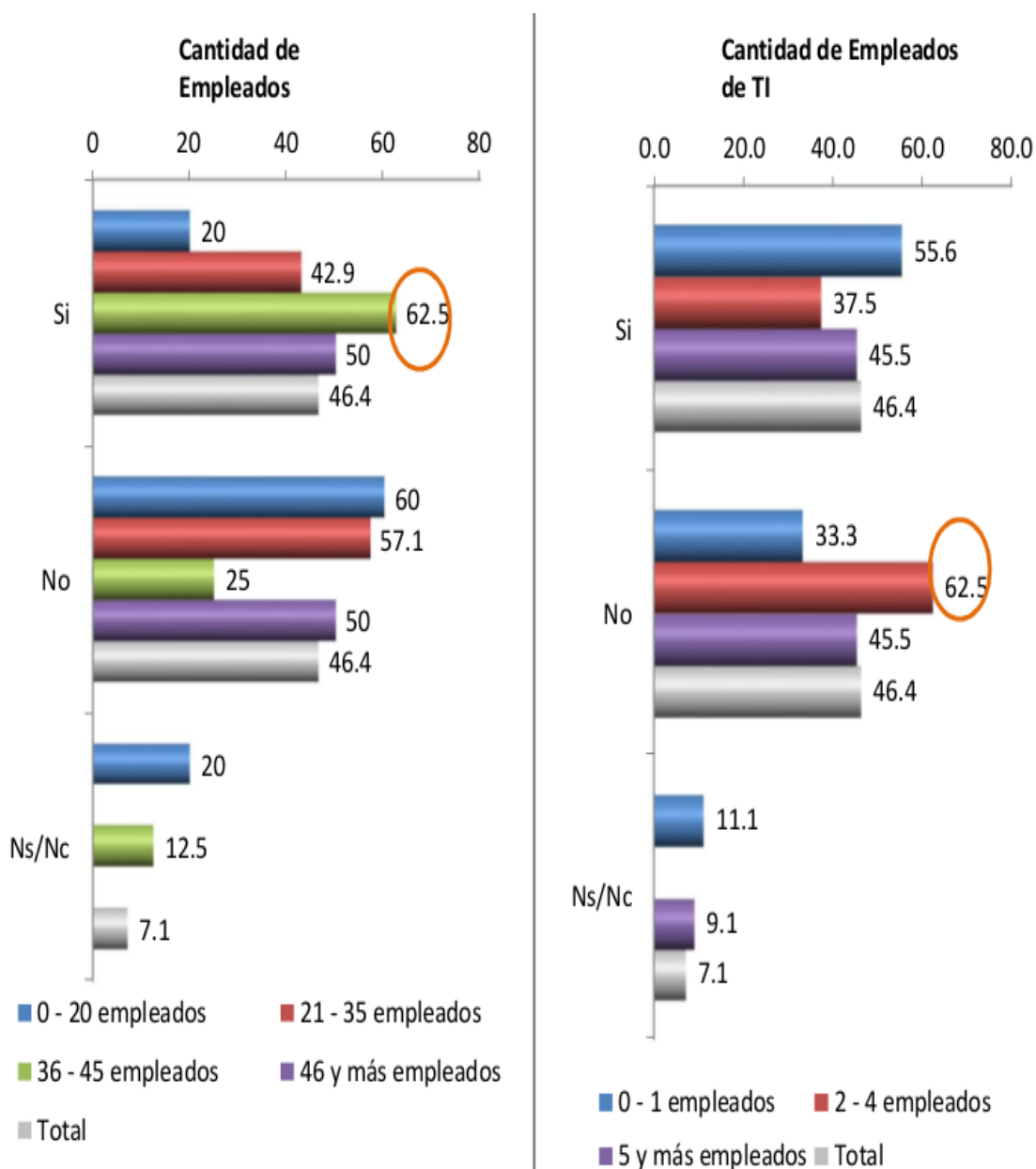


Cantidad de Empleados - A medida que aumenta la cantidad de personal se observan menos problemas en cuanto a deficiencias en conocimientos técnicos por parte del personal.

Cantidad de Empleados de TI - Las empresas con mayor cantidad de personal de TI son las que manifiestan mayores deficiencias en conocimiento técnico de su personal de TI.

2.6 Problemas experimentados en las TI los últimos 12 meses: Problemas de falta de agilidad en desarrollo/adquisición de aplicaciones según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 22. Problemas experimentados en las TI los últimos 12 meses: Problemas de falta de agilidad en desarrollo/adquisición de aplicaciones según cantidad de empleados y cantidad de empleados de TI



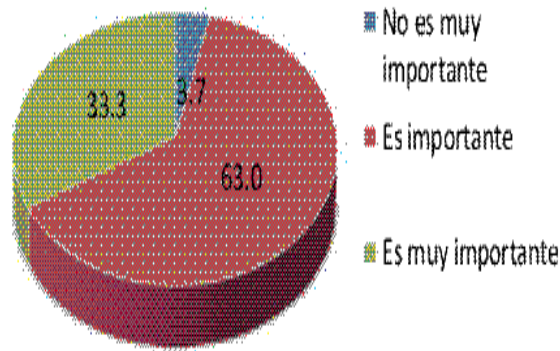
Cantidad de Empleados - Las empresas que tienen entre 36 y 45 empleados son las que manifiestan en mayor medida problemas de falta de agilidad en desarrollo y adquisición de aplicaciones.

Cantidad de Empleados de TI - Quienes manifiestan en menor medida haber sufrido este problema son las empresas que tienen de 2 a 4 empleados de TI.

3. APORTACIÓN DE VALOR

3.1 Importancia de la gestión de riesgo en su organización

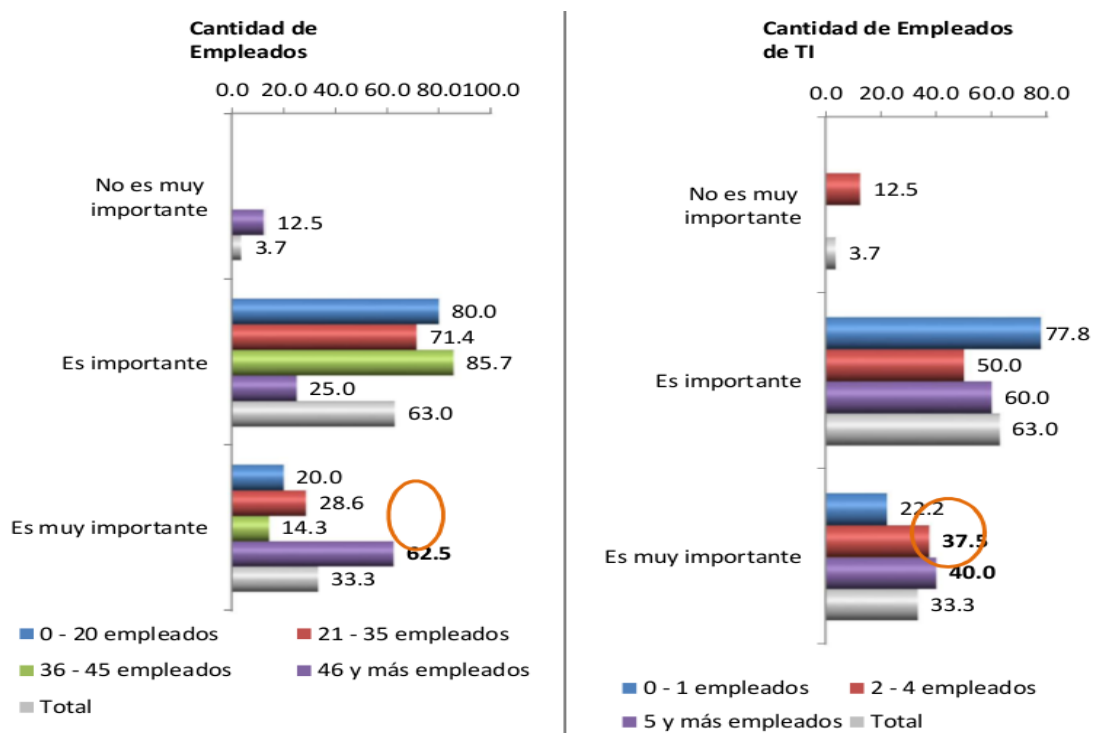
Grafica 23. ¿Qué importancia tiene la gestión de riesgos en su organización?



Para el 63% de las empresas consultadas, es importante la gestión de riesgo en su organización. El 33,3% considera que es muy importante la gestión de riesgo y el 3,7% expresa que no es muy importante esta gestión en su organización.

3.2 Importancia de la gestión de riesgo en su organización según Cantidad de Empleados y Cantidad de Empleados de TI

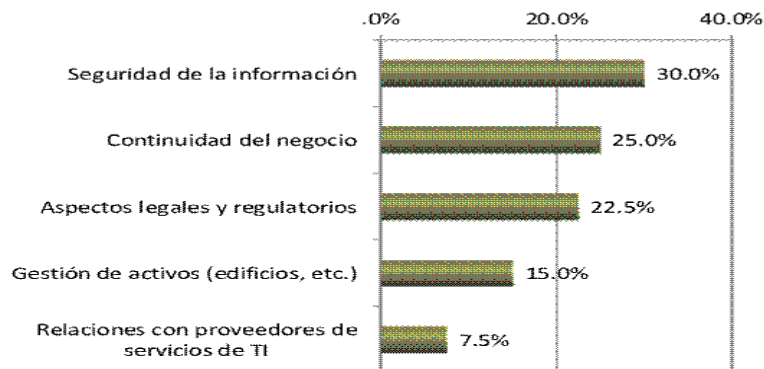
Grafica 24. ¿Qué importancia tiene la gestión de riesgos en su organización?



Cantidad de Empleados - Son las **Cantidad de Empleados de TI** - A empresas con mayor cantidad de medida que aumenta la cantidad de empleados las que manifiestan en mayor empleados de TI aumentas la importancia medida que la gestión de riesgos en su otorgada a la gestión del riesgo. organización es «muy importante»

3.3 Áreas en que se realiza la gestión de riesgo

Grafica 25. Indique, si se realiza una gestión de riesgos, y en qué áreas o aspectos se realiza



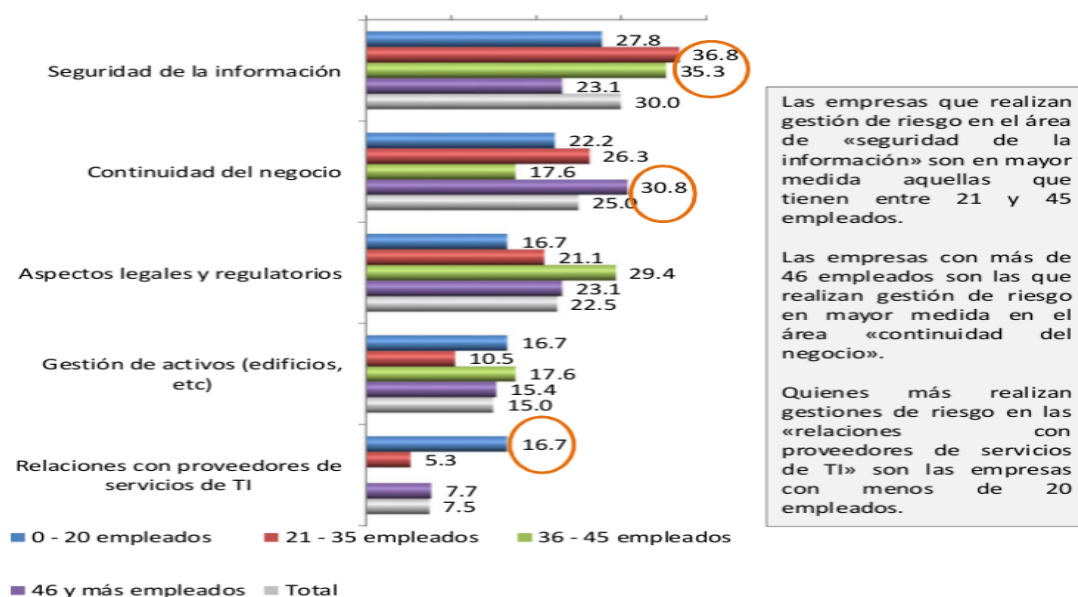
El 30% de las empresas consultadas realiza una gestión de riesgo en el área de seguridad de la información.

El 25% explica que realiza esta gestión en aspectos de continuidad del negocio y cuestiones legales-regulatorias.

Según el 15% la gestión de activos es una de las áreas donde se realiza la gestión de riesgo y para el restante 7,5% de los entrevistados la gestión se aplica a las relaciones con proveedores de servicio de TI.

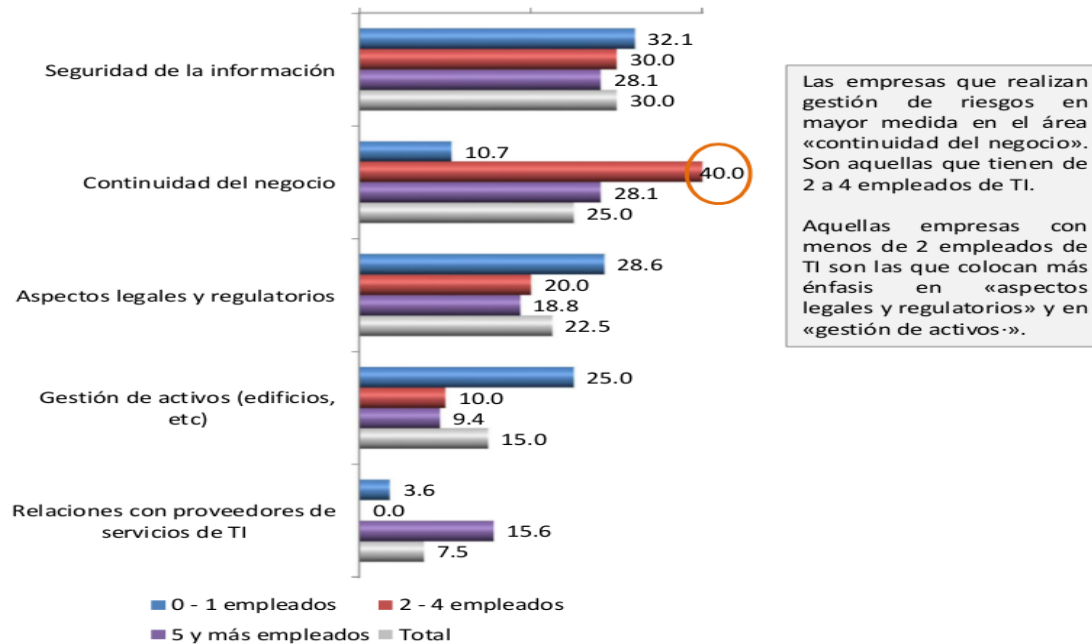
3.4 Áreas en que se realiza la gestión de riesgo según Cantidad de Empleados

Grafica 26. Indique, si se realiza una gestión de riesgos, y en qué áreas o aspectos se realiza



3.5 Áreas en que se realiza la gestión de riesgo según Cantidad de Empleados de TI

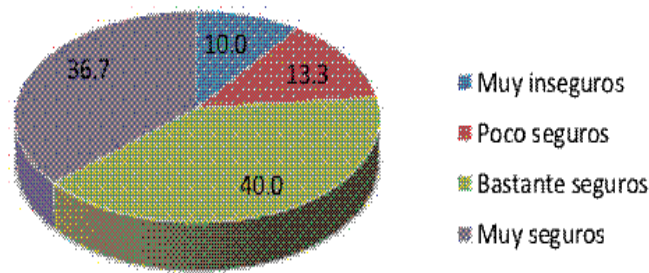
Grafica 27. Indique, si se realiza una gestión de riesgos, y en qué áreas o aspectos se realiza



4. SEGURIDAD

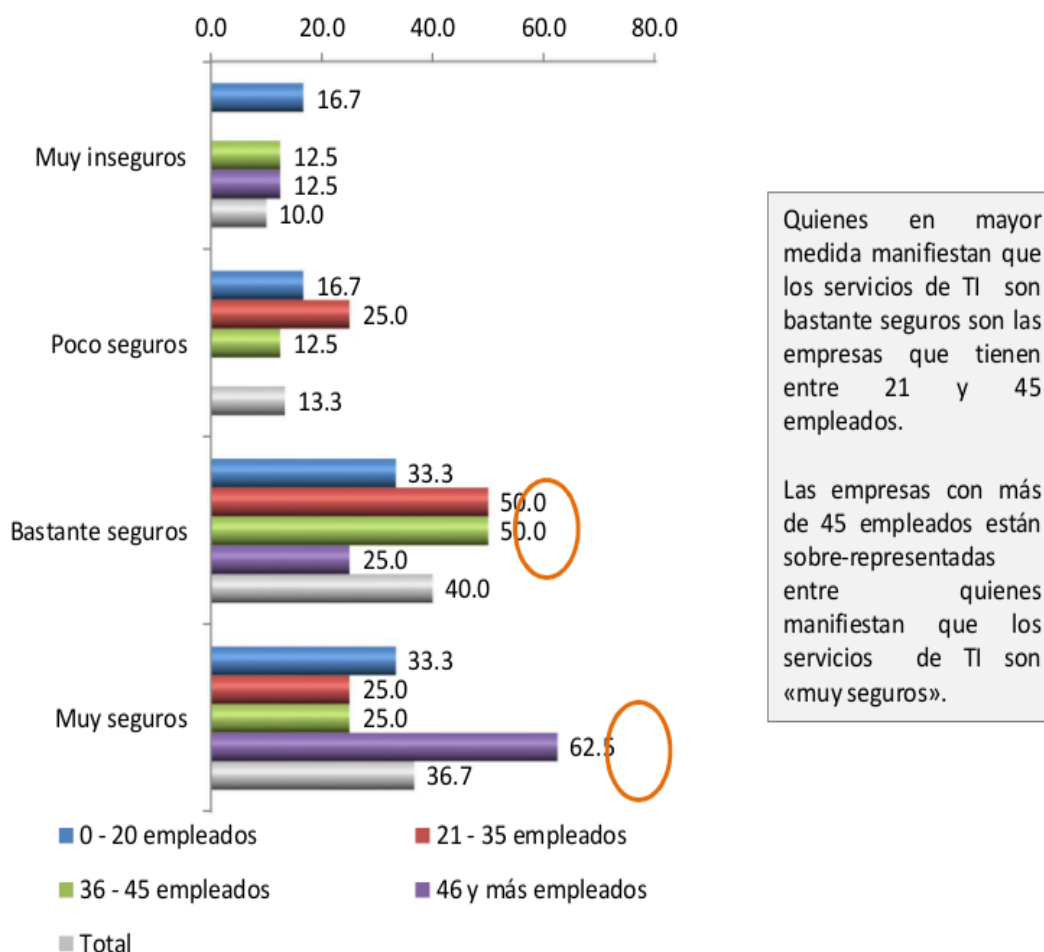
4.1 Valoración de la seguridad en general de los servicios de TI de su empresa

Grafica 28. ¿Cómo estima la seguridad en general de los servicios de TI de su empresa?



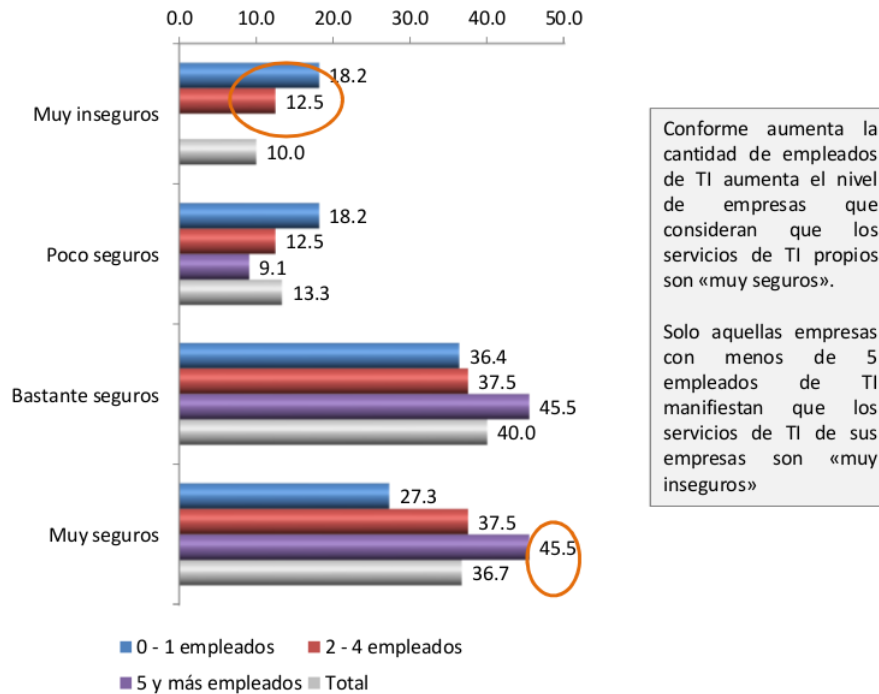
4.2 Valoración de la seguridad en general de los servicios de TI de su empresa según Cantidad de Empleados

Grafica 29. ¿Cómo estima la seguridad en general de los servicios de TI de su empresa?



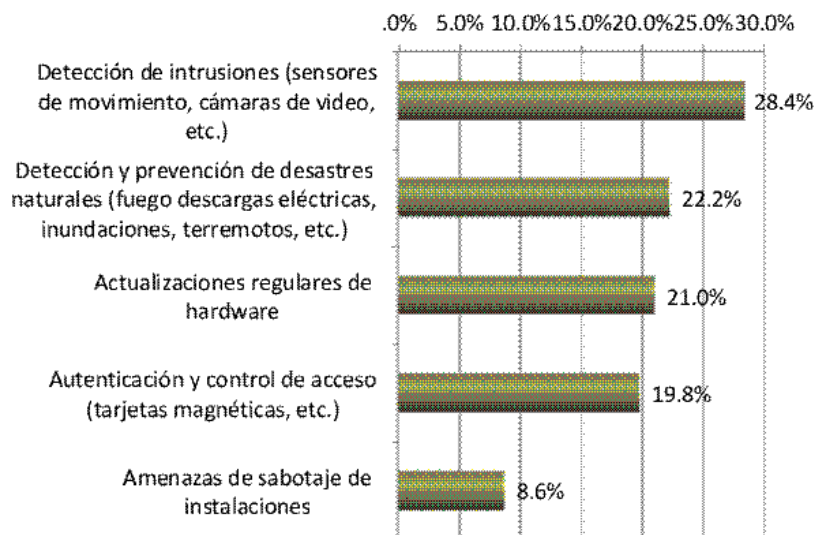
4.3 Valoración de la seguridad en general de los servicios de TI de su empresa según Cantidad de Empleados de TI

Grafica 30. ¿Cómo estima la seguridad en general de los servicios de TI de su empresa?



4.4 Tipo de seguridad física aplicable respecto a TI

Grafica 31. ¿Qué tipo de seguridad física aplica con respecto a TI?

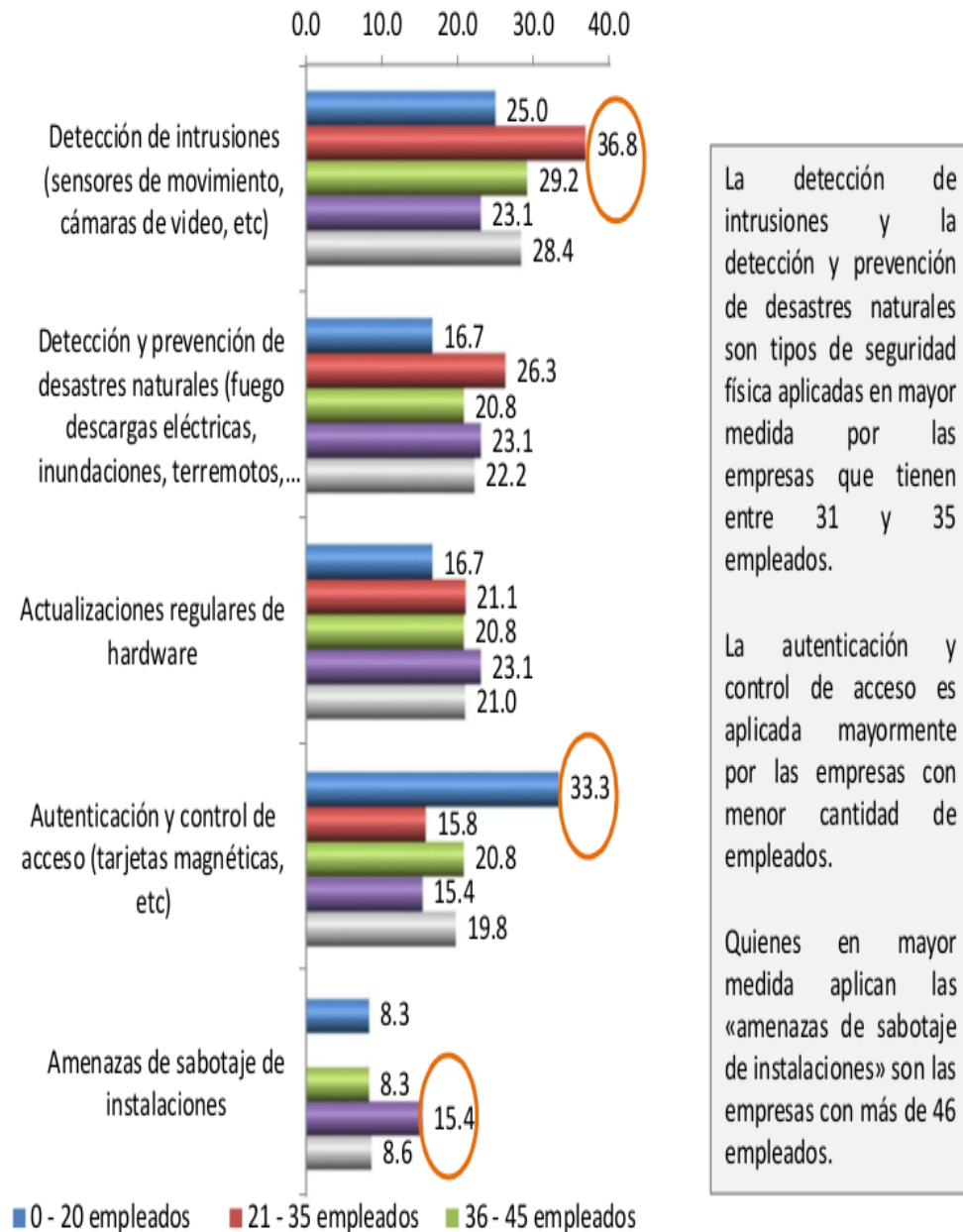


El 28,4% de las empresas aplica como medida de seguridad física la detección de intrusiones. El 22,2% utiliza la detección y prevención de desastres naturales.

Según el 21% de los entrevistados, la actualización regular de hardware es la medida que se aplica con respecto a TI . También la autenticación y control de acceso es un tipo de seguridad física que se aplica en el 19,8% de las empresas.

4.5 Tipo de seguridad física aplicable respecto a TI según Cantidad de Empleados

Grafica 32. ¿Qué tipo de seguridad física aplica con respecto a TI?



La detección de intrusiones y la detección y prevención de desastres naturales son tipos de seguridad física aplicadas en mayor medida por las empresas que tienen entre 31 y 35 empleados.

La autenticación y control de acceso es aplicada mayormente por las empresas con menor cantidad de empleados.

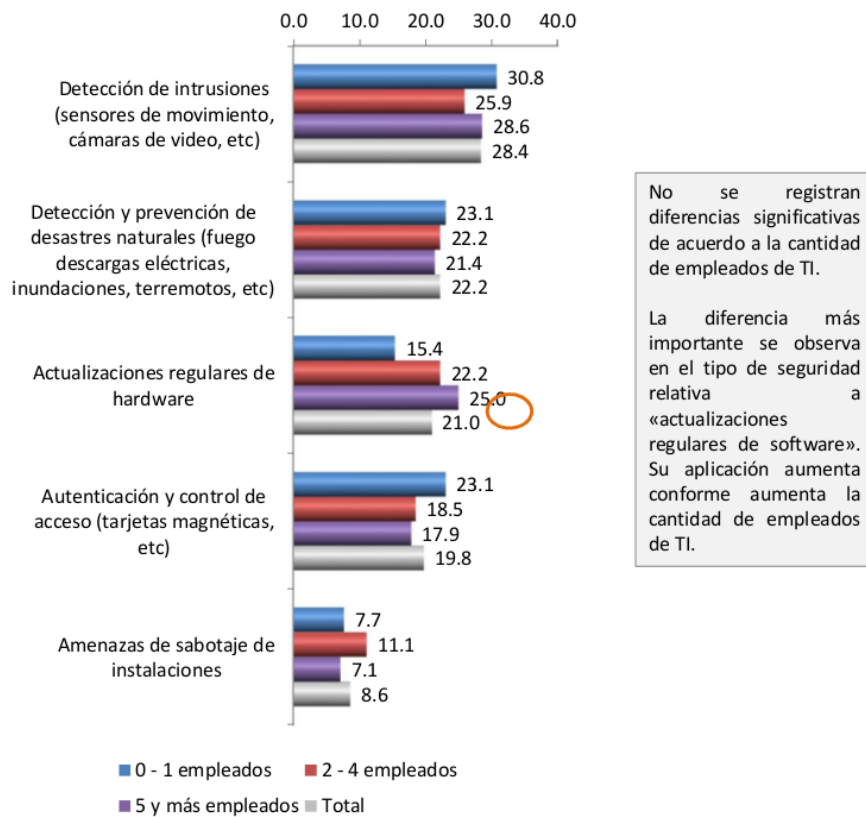
Quienes en mayor medida aplican las «amenazas de sabotaje de instalaciones» son las empresas con más de 46 empleados.

La detección de intrusiones y la detección y prevención de desastres naturales son tipos de seguridad física aplicadas en mayor medida por las empresas que tienen entre 31 y 35 empleados. La autenticación y control de acceso es aplicada mayormente por las empresas con menor cantidad de empleados.

Quienes en mayor medida aplican las «amenazas de sabotaje de instalaciones» son las empresas con más de 46 empleados.

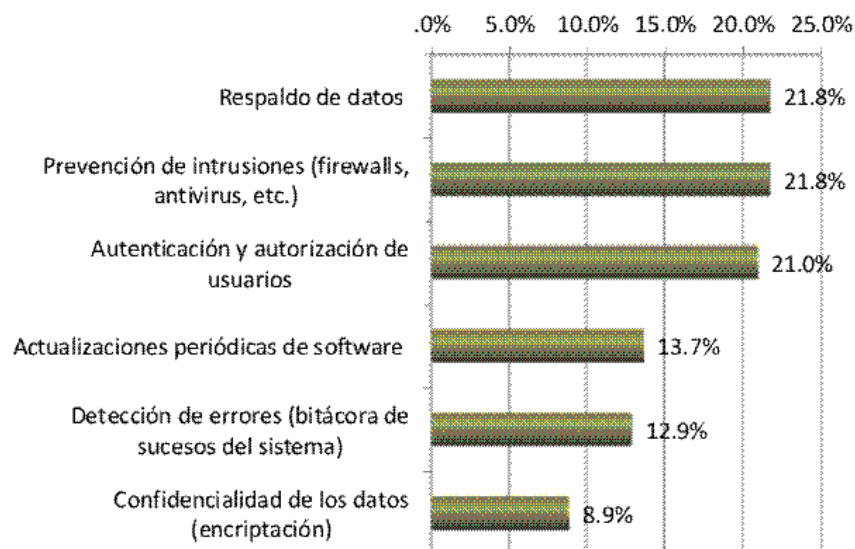
4.6 Tipo de seguridad física aplicable respecto a TI según Cantidad de Empleados de TI

Grafica 33. ¿Qué tipo de seguridad física aplica con respecto a TI?



4.7 Tipo de seguridad lógica aplicable respecto a la información de TI

Grafica 34. ¿Qué tipo de seguridad lógica aplica con respecto a la información de TI?

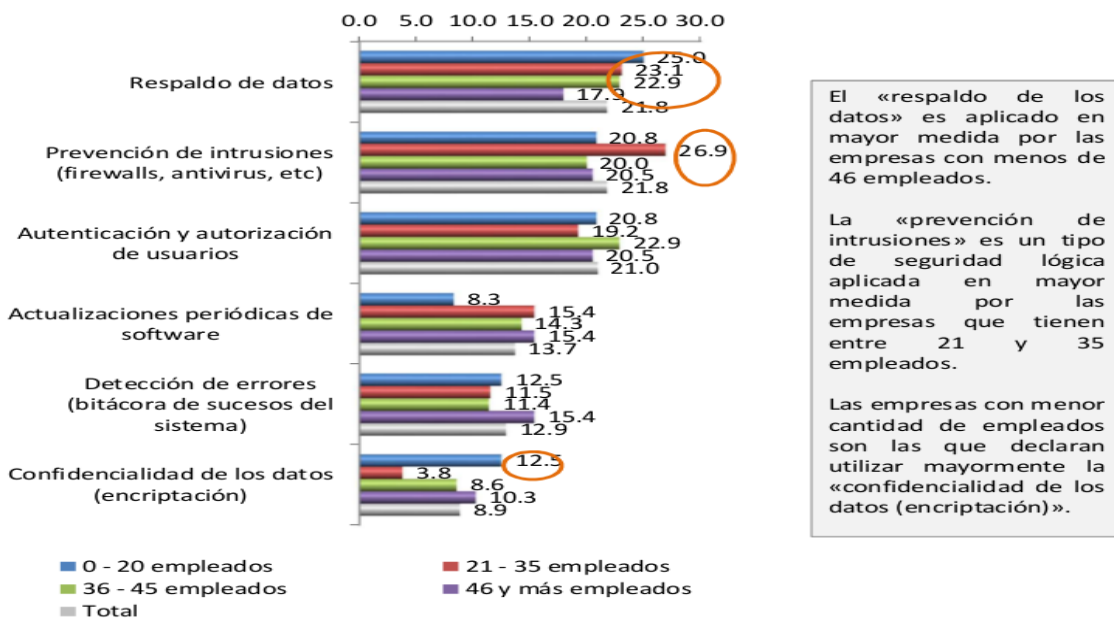


El tipo de seguridad lógica que más se aplica con respecto a la información de TI tiene que ver con el respaldo de datos y con la prevención de intrusiones.

Para el 21% de las empresas consultadas, la medida utilizada refiere a la autenticación y autorización de usuarios.

4.8 Tipo de seguridad lógica aplicable respecto a la información de TI según Cantidad de Empleados

Grafica 35. ¿Qué tipo de seguridad lógica aplica con respecto a la información de TI?



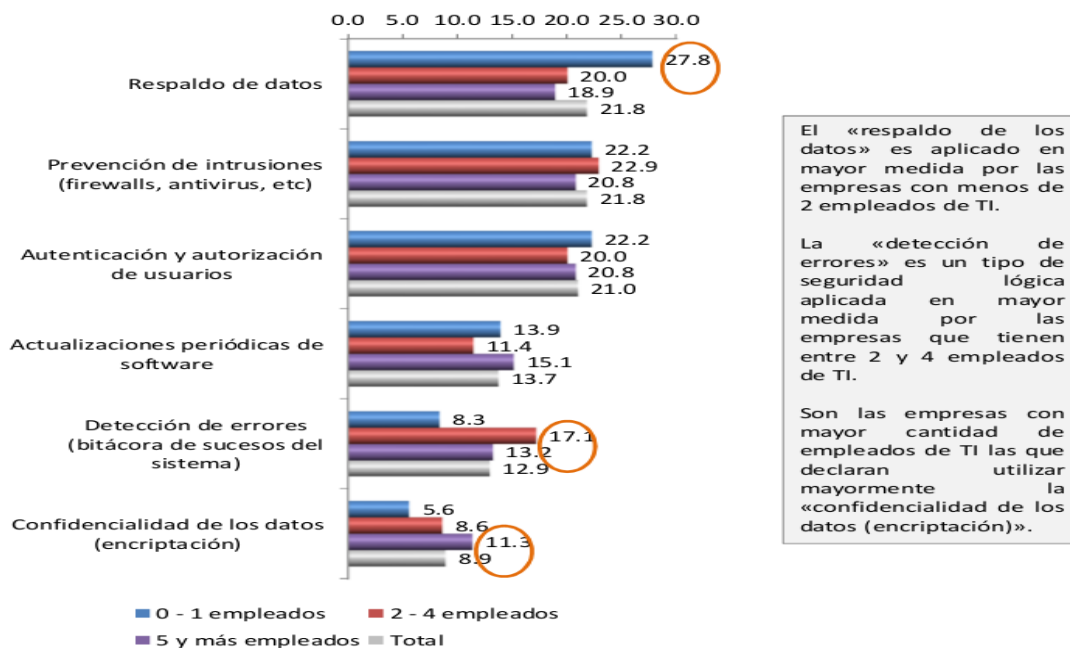
El «respaldo de los datos» es aplicado en mayor medida por las empresas con menos de 46 empleados.

La «prevención de intrusiones» es un tipo de seguridad lógica aplicada en mayor medida por las empresas que tienen entre 21 y 35 empleados.

Las empresas con menor cantidad de empleados son las que declaran utilizar mayormente la «confidencialidad de los datos (encriptación)».

4.9 Tipo de seguridad lógica aplicable respecto a la información de TI según Cantidad de Empleados de TI

Grafica 36. ¿Qué tipo de seguridad lógica aplica con respecto a la información de TI?



El «respaldo de los datos» es aplicado en mayor medida por las empresas con menos de 2 empleados de TI.

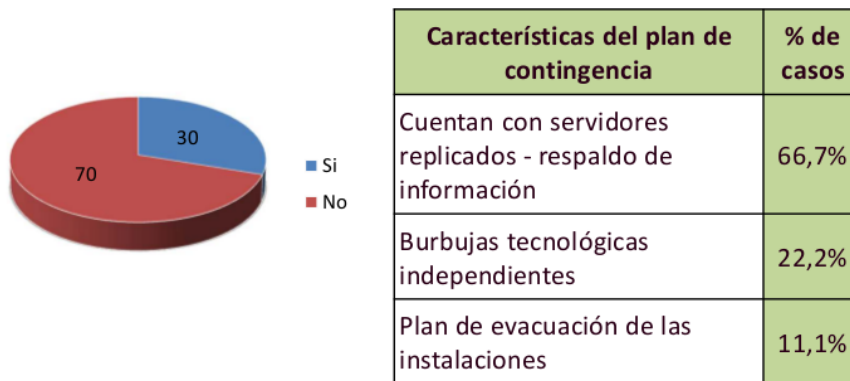
La «detección de errores» es un tipo de seguridad lógica aplicada en mayor medida por las empresas que tienen entre 2 y 4 empleados de TI.

Son las empresas con mayor cantidad de empleados de TI las que declaran utilizar mayormente la «confidencialidad de los datos (encriptación)».

4.10 Plan de recuperación de desastres

¿Cuenta con un plan de recuperación de desastres? En caso afirmativo explícite brevemente.

Gráfica 37. Cuenta con plan de recuperación de desastre



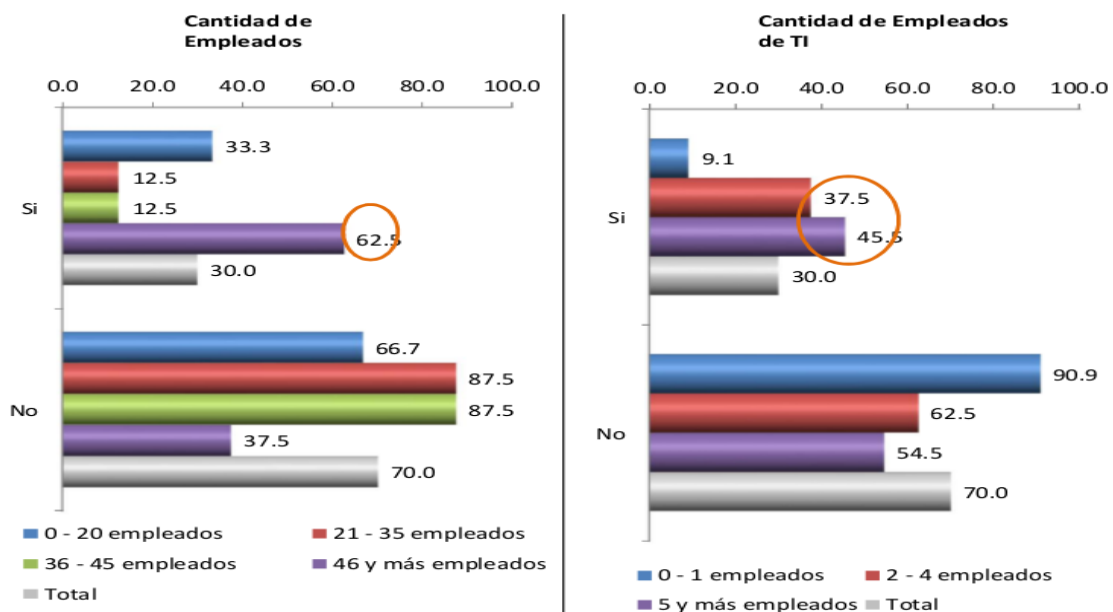
El 70% de las empresas no cuenta con un plan de recuperación de desastre. El restante 30% se caracteriza por si poseer un plan de contingencia.

De las empresas que poseen dicho plan, el 66,7% se caracteriza por ser un plan en donde se cuenta con servidores replicados.

Para el 22,2% de los entrevistados, el plan se define como burbujas tecnológicas independientes y según el 11,1% lo define como un plan de evacuación de las instalaciones.

4.11 Plan de recuperación de desastres según Cantidad de Empleados y Cantidad de Empleados de TI

Gráfica 38. ¿Cuenta con un plan de recuperación de desastres?

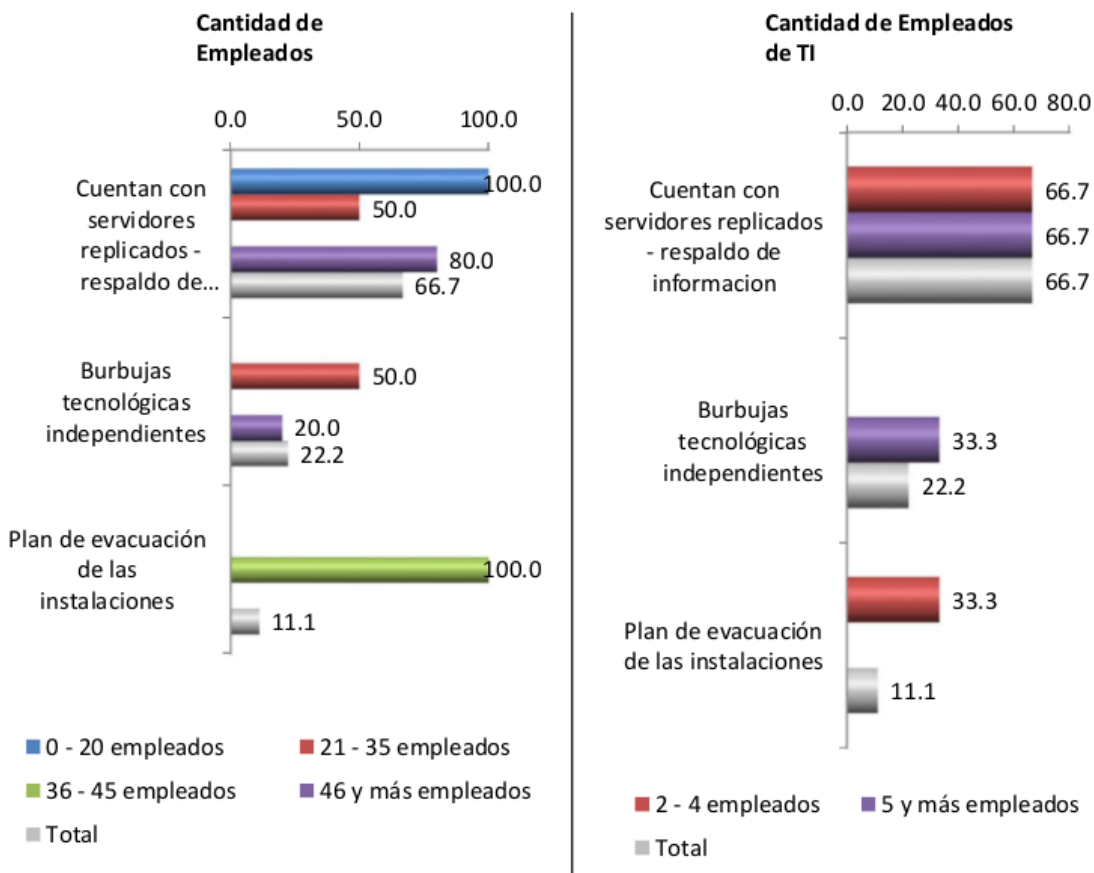


Cantidad de Empleados - Las empresas que en mayor medida cuentan con un plan de recuperación de desastres son aquellas que tienen más de 46 empleados.

Cantidad de Empleados de TI - Las empresas que en mayor medida cuentan con un plan de recuperación de desastres son aquellas que tienen más de 2 empleados de TI.

4.12 Plan de recuperación de desastres según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 39. Explicite cuál es el plan de recuperación de desastres con el que cuenta



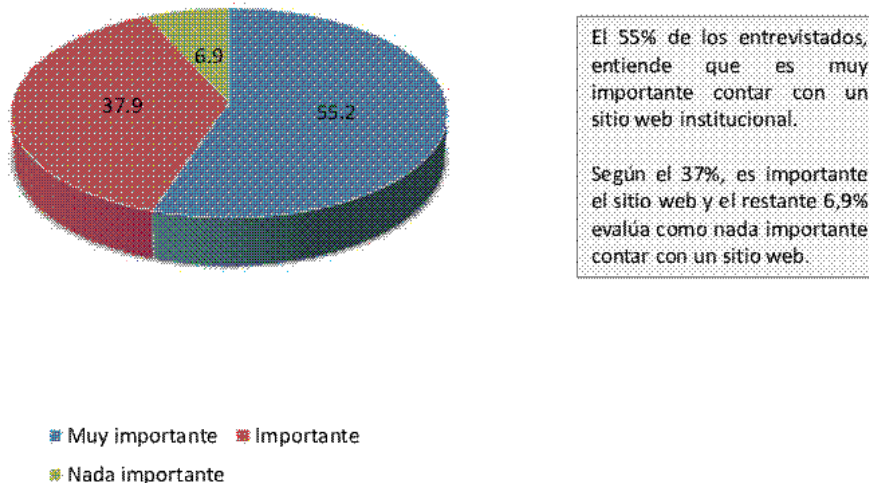
Cantidad de Empleados - Solo las empresas que tienen entre 36 y 45 empleados cuentan con un plan de evacuación de instalaciones. Las empresas con menos de 20 empleados solo cuentan con un plan de servidores replicados – respaldo de información.

Cantidad de Empleados de TI - La única empresa que tienen o a 1 empleado de TI manifestó no saber o no conocer cuál es el plan. Las «burbujas tecnológicas independientes» solo son utilizadas por las empresas con 5 o más empleados de TI

5. INTERNET

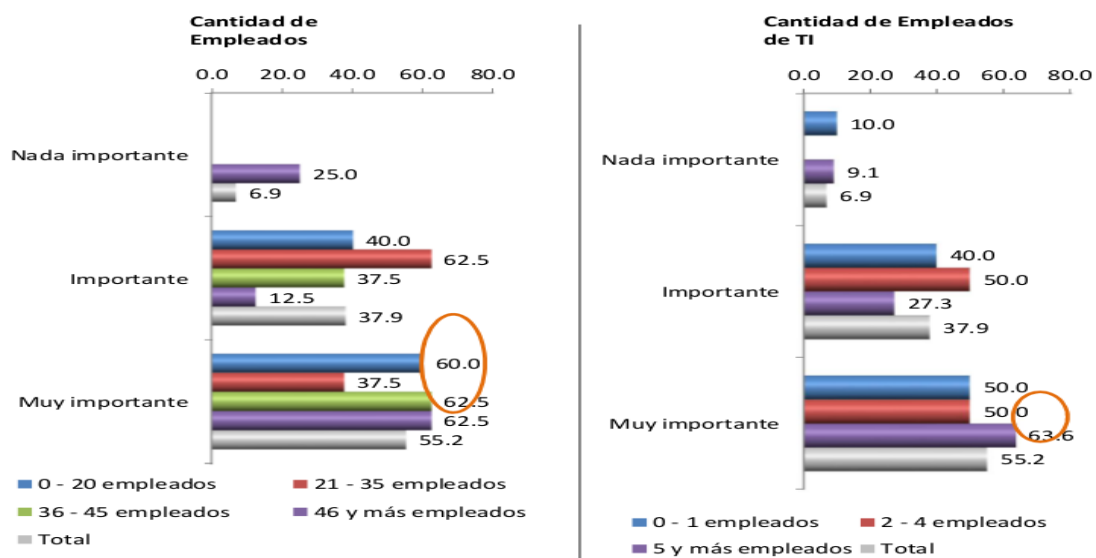
5.1 Importancia de contar con un sitio web institucional

Grafica 40. Importancia de sitio web



5.2 Importancia de contar con un sitio web institucional según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 41. ¿Cree que es importante el contar con un sitio web institucional?



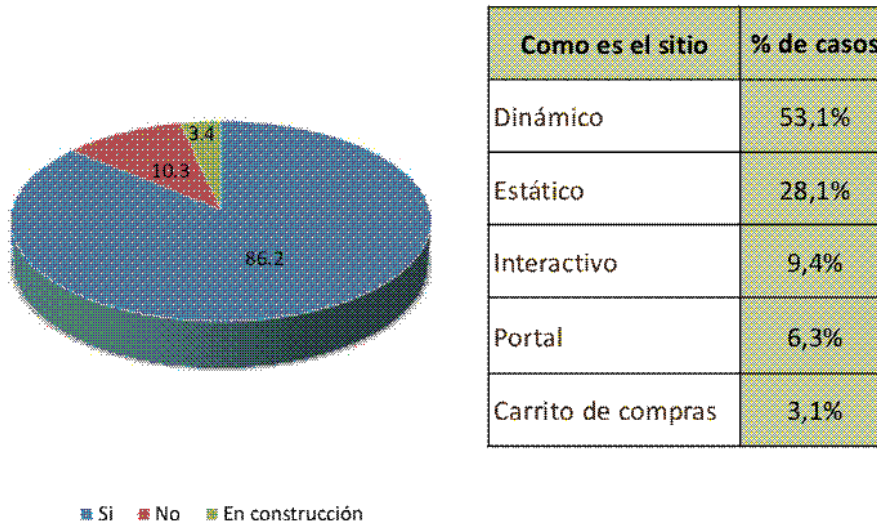
Cantidad de Empleados - Quienes en mayor medida consideran «muy importante» contar con un sitio web institucional son las empresas que tienen de 0 a 20 empleados y las que tienen más de 36 empleados.

Cantidad de Empleados de TI - Las empresas con más de 5 empleados de TI son las que manifiestan mayormente que es «muy importante» contar con un sitio web.

5.3 y 5.4 Cuenta con un sitio web y como es

¿Cuenta con un sitio Web institucional? Si tiene sitio web institucional ¿cómo es el sitio?

Grafica 42. Cuenta con un sitio web institucional

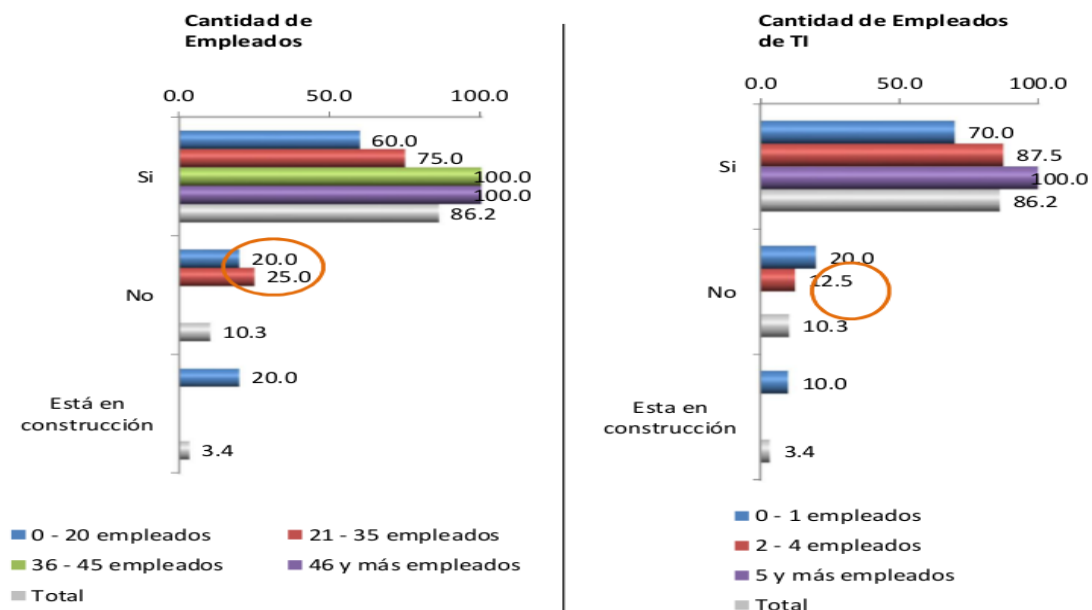


El 86,2% de las empresas cuenta con un sitio web institucional. El 10,3% no cuenta con el mismo y el 3,4% de los entrevistados expresa que el sitio está en construcción.

De aquellas empresas que cuenta con un sitio web, el 53,1% se caracteriza por ser dinámico y el 28,1 por ser estático.

5.5 Cuenta con un sitio web según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 43. ¿Cuenta con un sitio Web institucional? Si tiene sitio web institucional ¿cómo es el sitio?



Cantidad de Empleados - Solo las **Cantidad de Empleados de TI** – empresas con menos de 35 empleados Quienes manifiestan no contar con sitio manifiestan no contar con sitio web web institucional son las empresas con institucional. menos de 5 empleados de TI.

5.6 ¿Cómo es el sitio web?, según Cantidad de Empleados

	0 - 20 empleados	21 - 35 empleados	36 - 45 empleados	46 y más empleados	Total
Dinámico	80,0	57,1	36,4	55,6	53,1
Estático	0,0	14,3	45,5	33,3	28,1
Interactivo	0,0	14,3	9,1	11,1	9,4
Portal	0,0	14,3	9,1	0,0	6,3
Carrito de compras	20,0	0,0	0,0	0,0	3,1

Las empresas con menor cantidad de empleados son las que en mayor medida cuentan con un sitio web dinámico (80%).

Las empresas que cuentan con más de 36 empleados son las que en mayor medida tienen un sitio web estático.

Figura 4. Si tiene sitio web institucional ¿cómo es el sitio?

5.7 ¿Cómo es el sitio web?, según Cantidad de Empleados de TI

	0 - 1 empleados	2 - 4 empleados	5 y más empleados	Total
Dinámico	40,0	33,3	76,9	53,1
Estático	50,0	44,4	0,0	28,1
Interactivo	0,0	22,2	7,7	9,4
Portal	10,0	0,0	7,7	6,3
Carrito de compras	0,0	0,0	7,7	3,1

Las empresas que tienen más de 5 empleados de TI son las que en mayor medida cuentan con un sitio web dinámico (76,9%).

Las empresas que cuentan con menor cantidad de empleados de TI son las que en mayor medida tienen un sitio web estático.

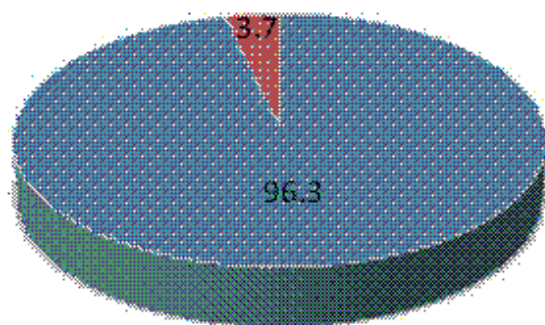
Figura 5. Cuenta con un sitio Web institucional? Si tiene sitio web institucional ¿cómo es el sitio?

5.8 Importancia del sitio web para apoyar y favorecer los objetivos estratégicos de la organización

¿Cree Ud. que el sitio web institucional apoya y favorece los objetivos estratégicos de la organización?

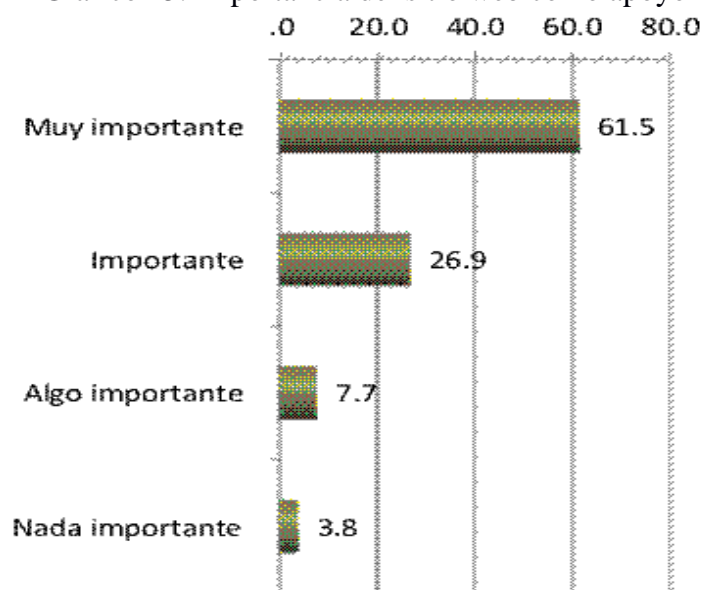
Si la respuesta es afirmativa ¿De qué manera?

Grafica 44. Sitio web como apoyo a los objetivos de la organización



■ Si ■ No

Grafico 45. Importancia del sitio web como apoyo

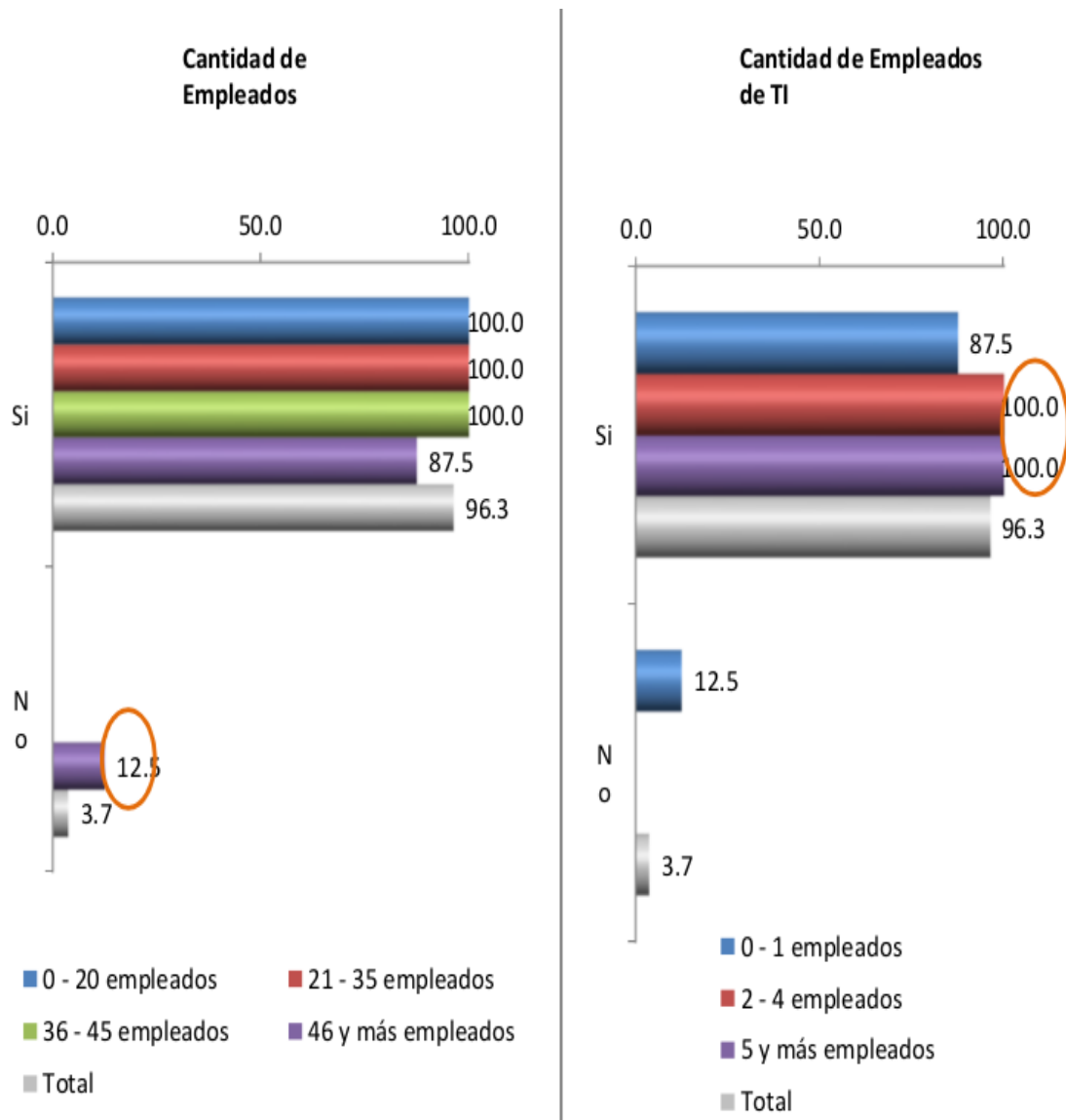


El 96,3% de los entrevistados, considera que el sitio web institucional apoya y favorece los objetivos estratégicos de la organización.

Para el 61,5% es muy importante el apoyo a los objetivos de la organización. El 26,9% considera que es importante y el 7,7% evalúa como algo importante el sitio web como apoyo a la estrategia de la organización.

5.9 Importancia del sitio web para apoyar y favorecer los objetivos estratégicos de la organización según Cantidad de Empleados y Cantidad de Empleados de TI

Grafico 46. ¿Cree Ud. que el sitio web institucional apoya y favorece los objetivos estratégicos de la organización? Si la respuesta es afirmativa ¿De qué manera?



Cantidad de Empleados - Solo entre las empresas con más de 46 empleados se registran un nivel de menciones negativas acerca de la importancia del sitio web para apoyar y favorecer los objetivos estratégicos de la organización.

Cantidad de Empleados de TI - La totalidad de las empresas con más de 2 empleados de TI manifiestan que el sitio web apoya y favorece los objetivos estratégicos de la organización.

5.10 Utilidad, beneficio y valor que aporta el sitio web

Utilidad que aporta el sitio web	% de casos
Acceso a información genérica de la empresa por parte de potenciales clientes	40,5%
Presencia en el mercado	37,8%
Información general	5,4%
Facilidad operativa	5,4%
Mejora la gestión de datos	5,4%
Interacción con los alumnos	2,7%
Clientes pueden ver información de la mercadería entregada	2,7%

Figura 6. ¿Qué utilidad, beneficios y valor le aporta el sitio web?

5.11 Utilidad, beneficio y valor que aporta el sitio web según Cantidad de Empleados

	0 - 20 empleados	21 - 35 empleados	36 - 45 empleados	46 y más empleados	Total
Acceso a información genérica de la empresa por parte de potenciales clientes	33,3	54,5	35,7	33,3	40,5
Presencia en el mercado	50,0	27,3	42,9	33,3	37,8
Información general	0,0	0,0	14,3	0,0	5,4
Facilidad operativa	0,0	9,1	0,0	16,7	5,4
Mejora la gestión de datos	16,7	0,0	7,1		5,4
Interacción con los alumnos	0,0	9,1	0,0	0,0	2,7
Clientes pueden ver					

Figura 7. ¿Qué utilidad, beneficios y valor le aporta el sitio web?

5.12 Utilidad, beneficio y valor que aporta el sitio web según Cantidad de Empleados de TI

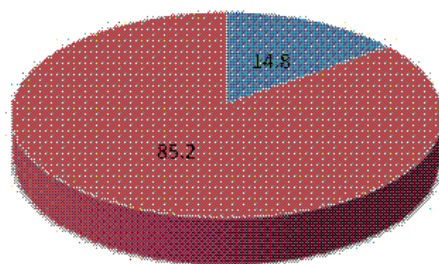
	0 - 1 empleados	2 - 4 empleados	5 y más empleados	Total
Acceso a información genérica de la empresa por parte de potenciales clientes	30,0	41,7	46,7	40,5
Presencia en el mercado	50,0	33,3	33,3	37,8
información general	10,0	0,0	6,7	5,4
Facilidad operativa	0,0	8,3	6,7	5,4
Mejora la gestión de datos	10,0	0,0	6,7	5,4
Interacción con los alumnos	0,0	8,3	0,0	2,7
Clientes pueden ver información de la mercadería entregada	0,0	8,3	0,0	2,7

Figura 8. ¿Qué utilidad, beneficios y valor le aporta el sitio web?

5.13 Problema en relación a un acceso indebido a la información

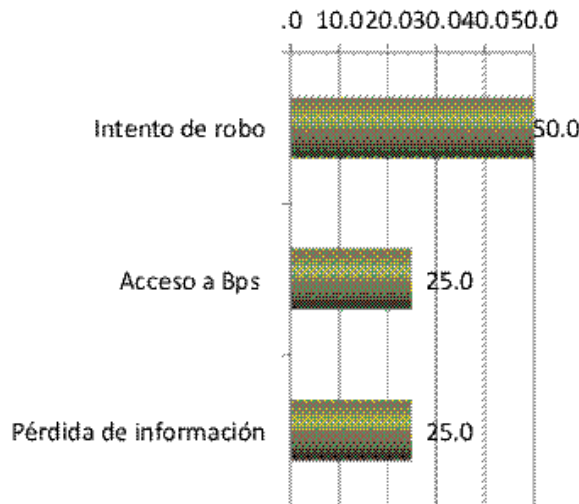
¿Ha sufrido algún problema en relación a un acceso indebido a la información? ¿Qué tipo de problema?

Grafica 47. ¿Ha tenido problema en relación a acceso indebido a la información?



■ Sí ■ No

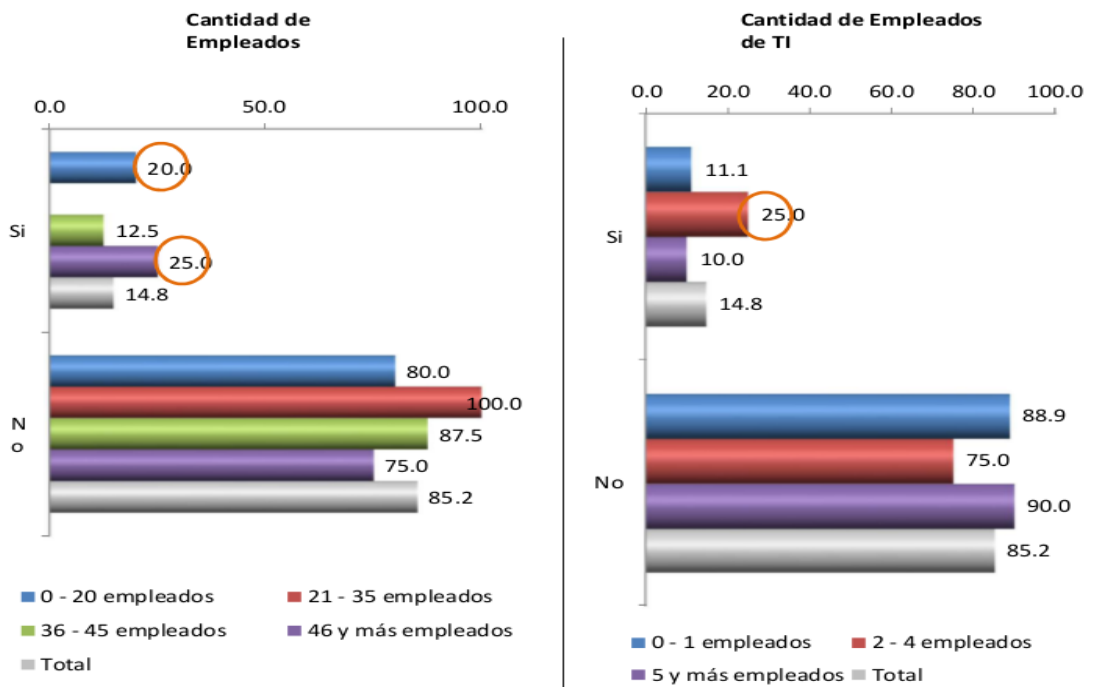
Grafica 48. Tipo de problema



El 85% de las empresas consultadas expresa que no ha tenido problemas en relación a acceso indebido a la información. El 14,8% manifiesta que si ha tenido este tipo de problemas. De las empresas que han tenido problema, el 50% tienen que ver con intento de robo, el 25% refiere a problemas en el acceso a BPS y el restante 25% refiere a pérdida de información.

5.14 Problema en relación a un acceso indebido a la información según Cantidad de Empleados

Grafica 49. ¿Ha sufrido algún problema en relación a un acceso indebido a la información? ¿Qué tipo de problema?

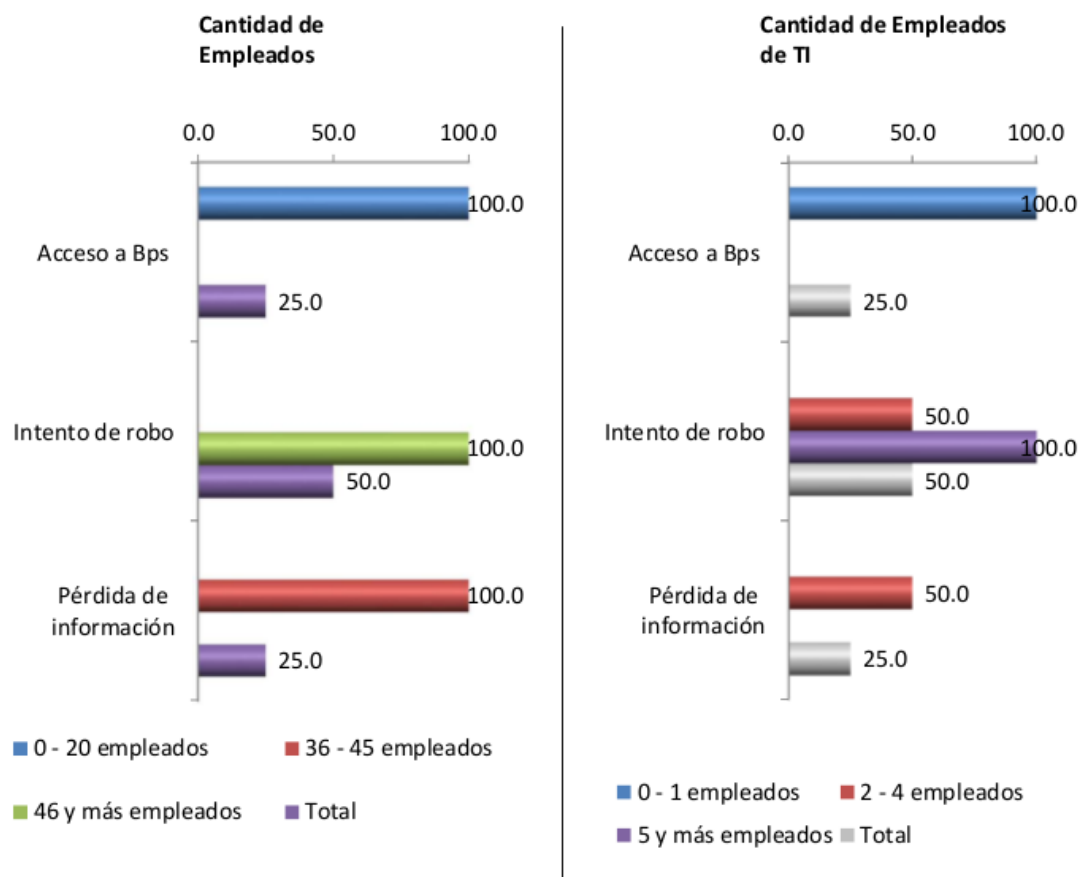


Cantidad de Empleados - Las empresas que manifiestan en mayor medida haber sufrido algún problema en relación a un acceso indebido a la información son aquellas que tienen menos de 20 empleados y más de 46.

Cantidad de Empleados de TI - Las empresas que manifiestan en mayor medida haber sufrido algún problema en relación a un acceso indebido a la información son aquellas que cuentan con 2 a 4 empleados de TI.

5.15 Problema en relación a un acceso indebido a la información según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 50. ¿Qué tipo de problema ha tenido en relación a un acceso indebido a la información?



Cantidad de Empleados - El principal problema sufrido por las empresas con menor cantidad de empleados es el acceso a Bps.

Las empresas con más de 46 empleados manifiestan haber sufrido principalmente «intento de robo».

Cantidad de Empleados de TI - Las empresas con 0 o 1 empleado de TI manifiestan haber sufrido un problema de «acceso a Bps».

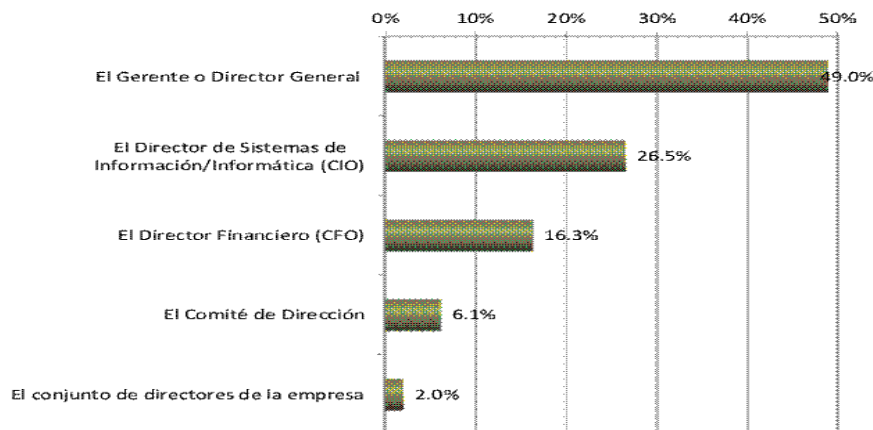
Las empresas con 5 o más empleados manifiestan haber sufrido principalmente «intento de robo».

6. TOMA DE DECISIONES

6.1 Toma de decisiones sobre TI en la organización

¿Quién toma las decisiones sobre TI en su organización?

Grafica 51. Toma de decisiones sobre TI

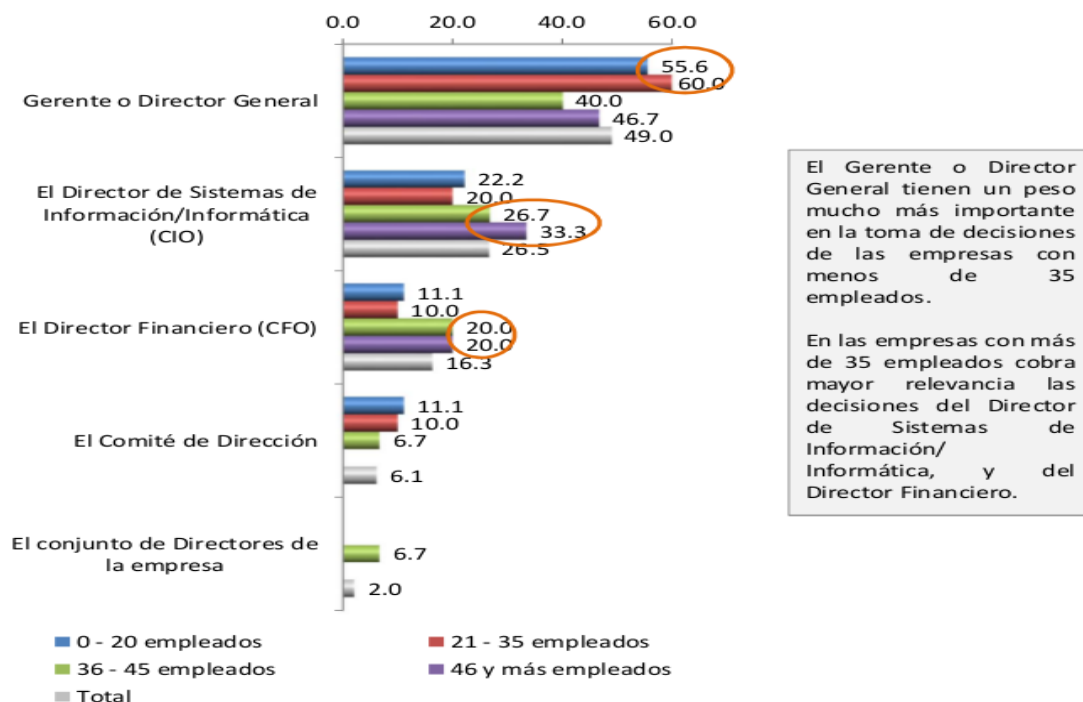


En el 49% de las empresas quien toma las decisiones sobre TI es el gerente o director general. El 26% de los entrevistados, explica que es el director de sistemas de información quien toma las decisiones.

Y para el 16,3% de las empresas quien toma las decisiones es el director financiero.

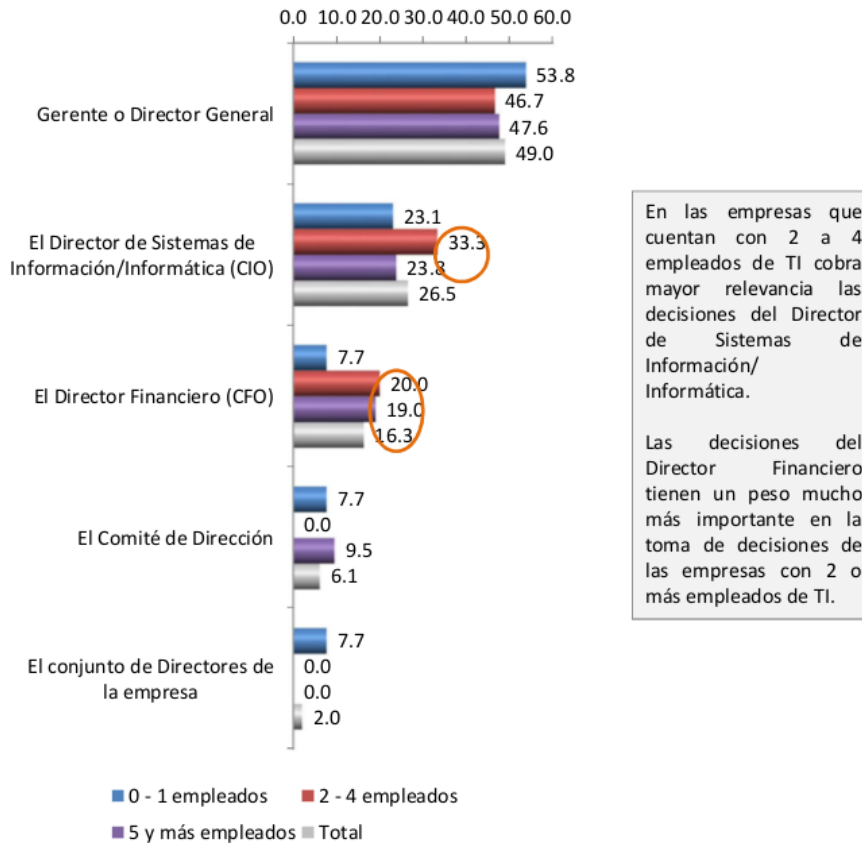
6.2 Toma de decisiones sobre TI en la organización según Cantidad de Empleados

Grafica 52. ¿Quién toma las decisiones sobre TI en su organización?



6.3 Toma de decisiones sobre TI en la organización según Cantidad de Empleados de TI

Grafica 53. ¿Quién toma las decisiones sobre TI en su organización?



6.4 Nivel de implicación de la gestión del negocio en el gobierno de las iniciativas de TI asociadas al negocio

¿Cómo describiría el nivel de implicación de la gestión del negocio en el gobierno de las iniciativas de TI asociadas al negocio?

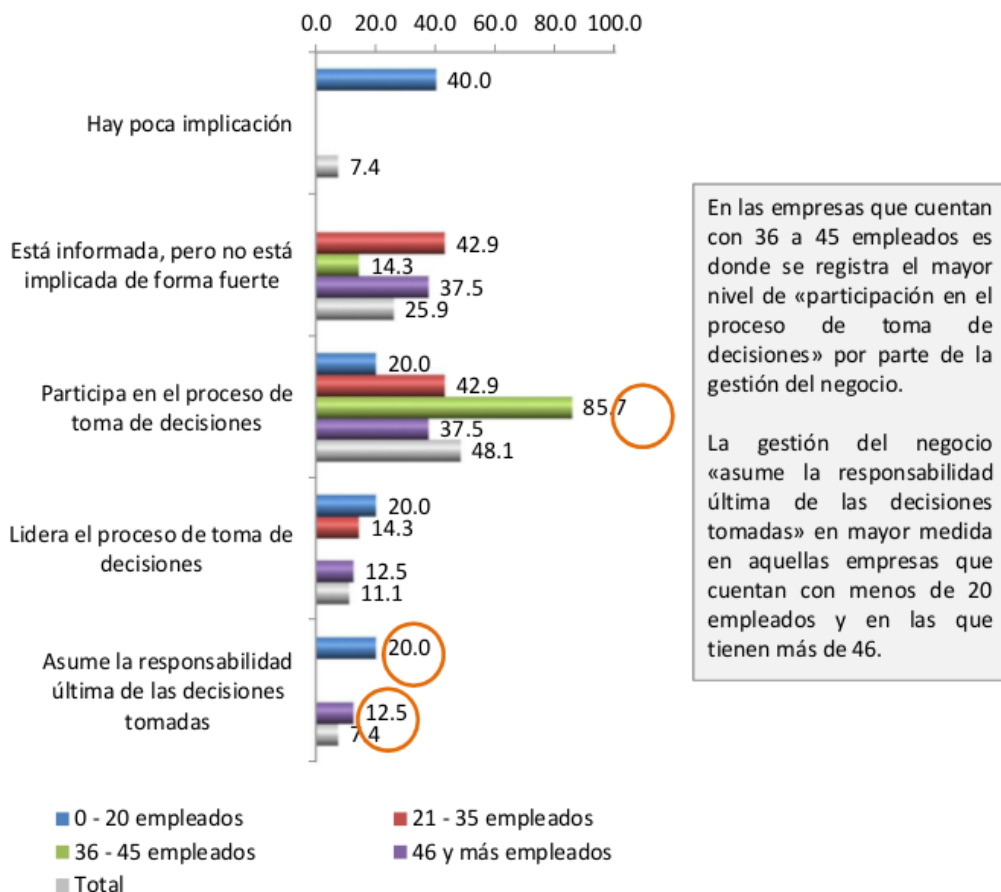
Grafica 54. Nivel de implicación de la gestión del negocio en el gobierno de TI



El 48% de las empresas, participa en el proceso de toma de decisiones. El 25% expresa que está informada, pero no está implicada de forma fuerte en el gobierno de TI. Y el 11% de los casos, lidera el proceso de toma de decisiones.

6.5 Nivel de implicación de la gestión del negocio en el gobierno de las iniciativas de TI asociadas al negocio según Cantidad de Empleados

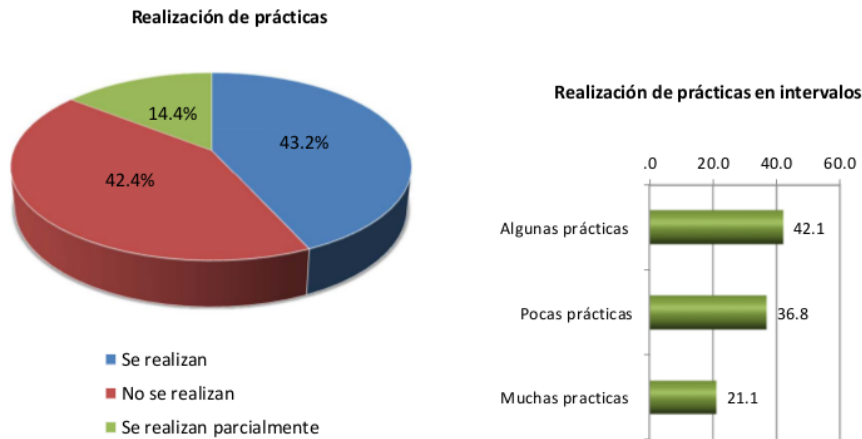
Grafica 55. ¿Cómo describiría el nivel de implicación de la gestión del negocio en el gobierno de las iniciativas de TI asociadas al negocio?



7. GOBIERNO DE LAS TI

7.1.1 Realización de prácticas asociadas con el gobierno de las TI

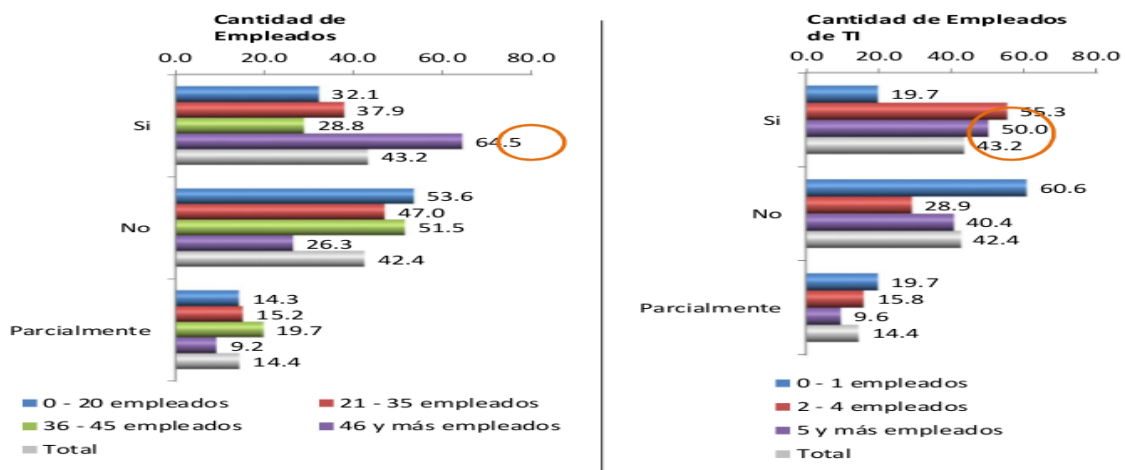
Grafica 56. ¿Se realizan alguna de las prácticas siguientes asociadas con el Gobierno de las TI en su organización?



El 43% de las empresas consultadas, realizan prácticas asociadas con el gobierno de TI. El 42% expresa que no realiza estas prácticas y el restante 14% explica que las realiza parcialmente. En relación a la cantidad de prácticas que se realizan, puede verse que el 42% realiza algunas prácticas y el 36% se caracteriza por efectuar pocas prácticas. Y el restante 21% expresa que realiza muchas prácticas asociadas con el gobierno de las Ti en su organización.

7.1.2 Realización de prácticas asociadas con el gobierno de las TI según Cantidad de Empleados

Grafica 57. ¿Se realizan alguna de las prácticas siguientes asociadas con el Gobierno de las TI en su organización?

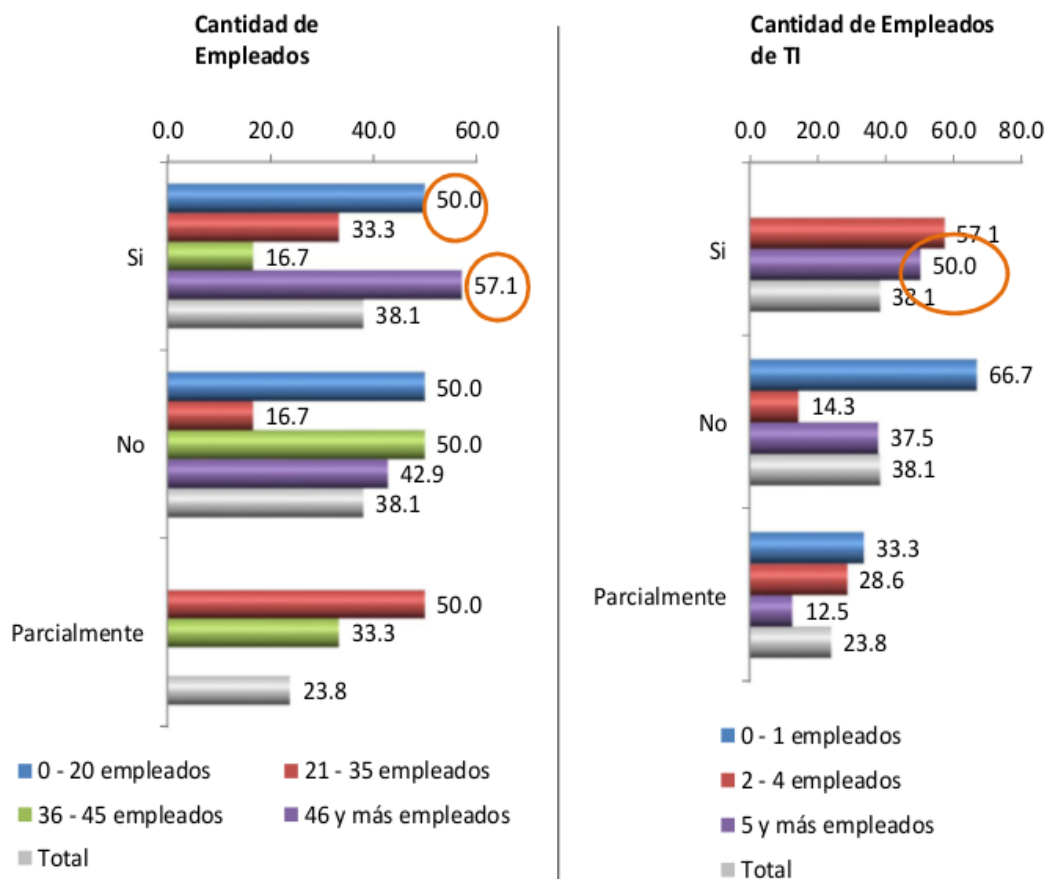


Cantidad de Empleados - Quienes en mayor medida manifiestan realizar prácticas asociadas con el gobierno de las TI son las empresas con más de 46 empleados.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan realizar prácticas asociadas con el gobierno de las TI son las empresas con 2 o más empleados.

7.1.3 Realización de prácticas asociadas con el gobierno de las TI: Establecer las estructuras organizativas adecuadas para supervisar y dirigir todos los recursos de TI de la organización según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 58. Realización de prácticas asociadas con el gobierno de las TI: Establecer las estructuras organizativas adecuadas para supervisar y dirigir todos los recursos de TI de la organización según cantidad de empleados y cantidad de empleados de TI

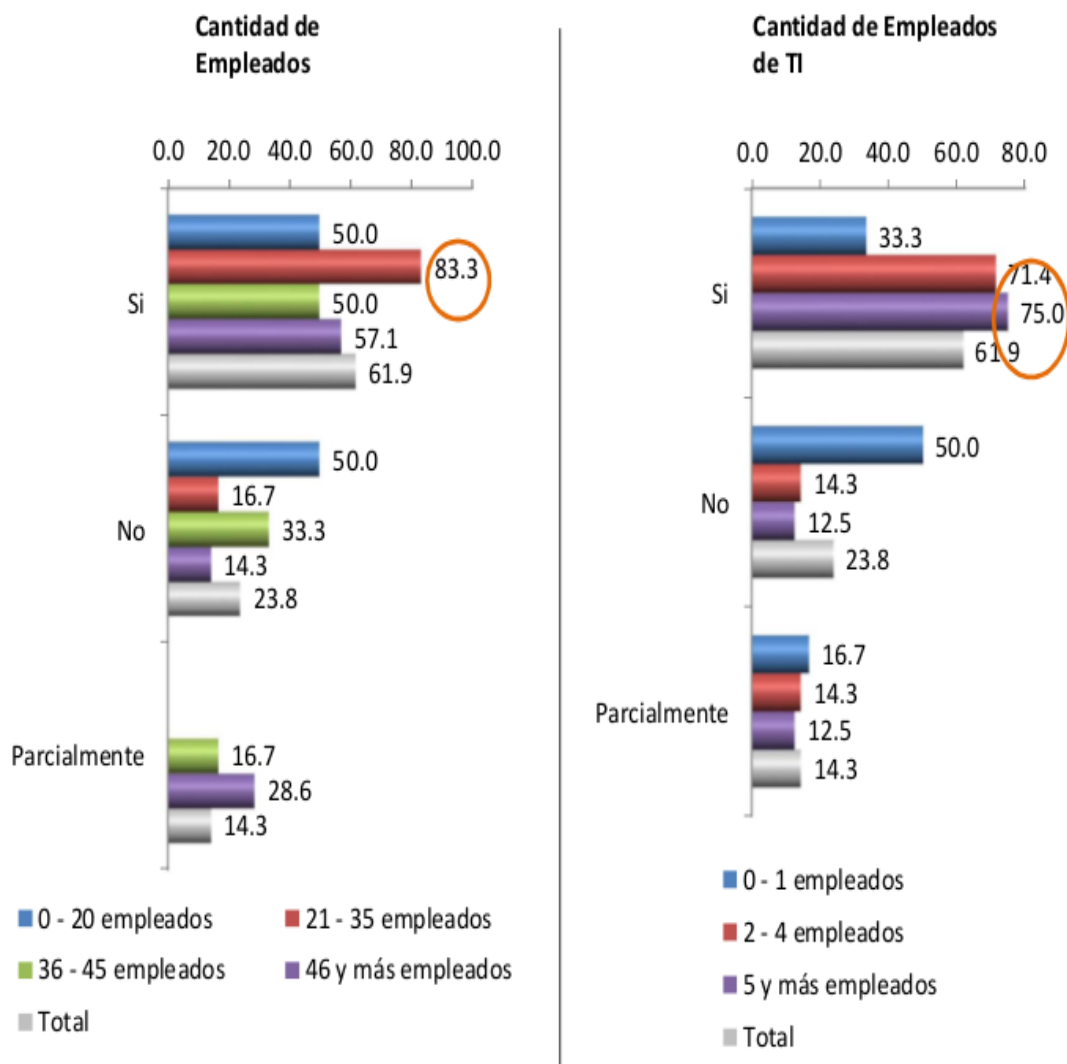


Cantidad de Empleados - Quienes en mayor medida manifiestan establecer las estructuras adecuadas para supervisar y dirigir los recursos de TI de su organización son las empresas con menos de 20 empleados y aquellas que tienen más de 46.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan establecer las estructuras adecuadas para supervisar y dirigir los recursos de TI de su organización son las empresas con 2 o más empleados de TI.

7.1.4 Realización de prácticas asociadas con el gobierno de las TI: El Consejo de Administración/Comité de Dirección revisa los presupuestos y los planes de TI de forma periódica según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 59. Realización de prácticas asociadas con el gobierno de las TI: El Consejo de Administración/Comité de Dirección revisa los presupuestos y los planes de TI de forma periódica según Cantidad de Empleados y Cantidad de Empleados de TI

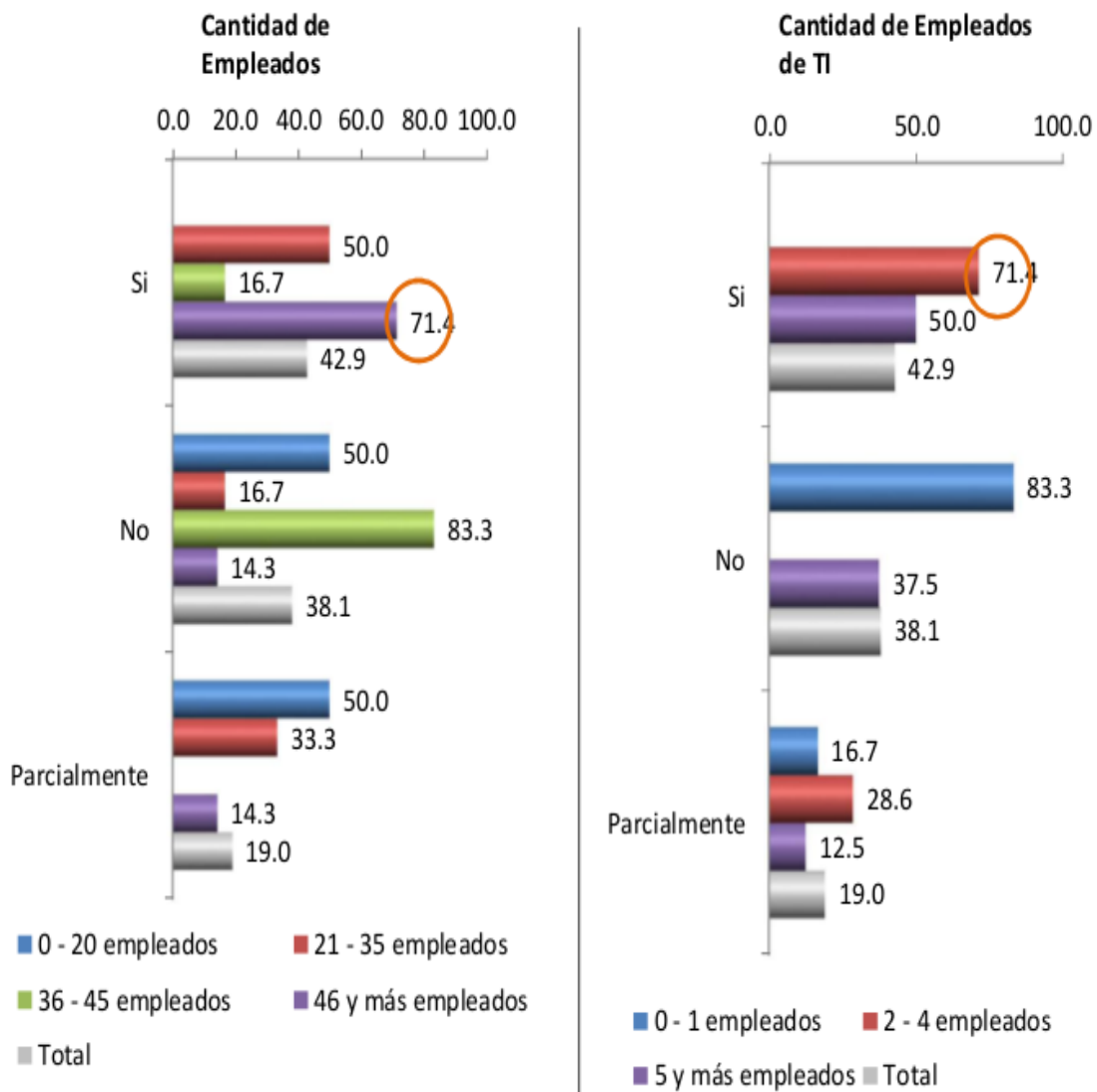


Cantidad de Empleados - Quienes en mayor medida manifiestan tener una supervisión de los presupuestos y planes de TI por parte del Consejo de administración/comité de dirección son las empresas que tienen entre 31 y 35 empleados.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan tener una supervisión de los presupuestos y planes de I por parte del Consejo de administración/comité de dirección son las empresas que tienen 2 o más empleados de TI.

7.1.5 Realización de prácticas asociadas con el gobierno de las TI: La cartera de proyectos de TI se gestiona por los departamentos de la organización, con la ayuda del departamento de TI según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 60. Realización de prácticas asociadas con el gobierno de las TI: La cartera de proyectos de TI se gestiona por los departamentos de la organización, con la ayuda del departamento de TI según Cantidad de Empleados y Cantidad de Empleados de TI

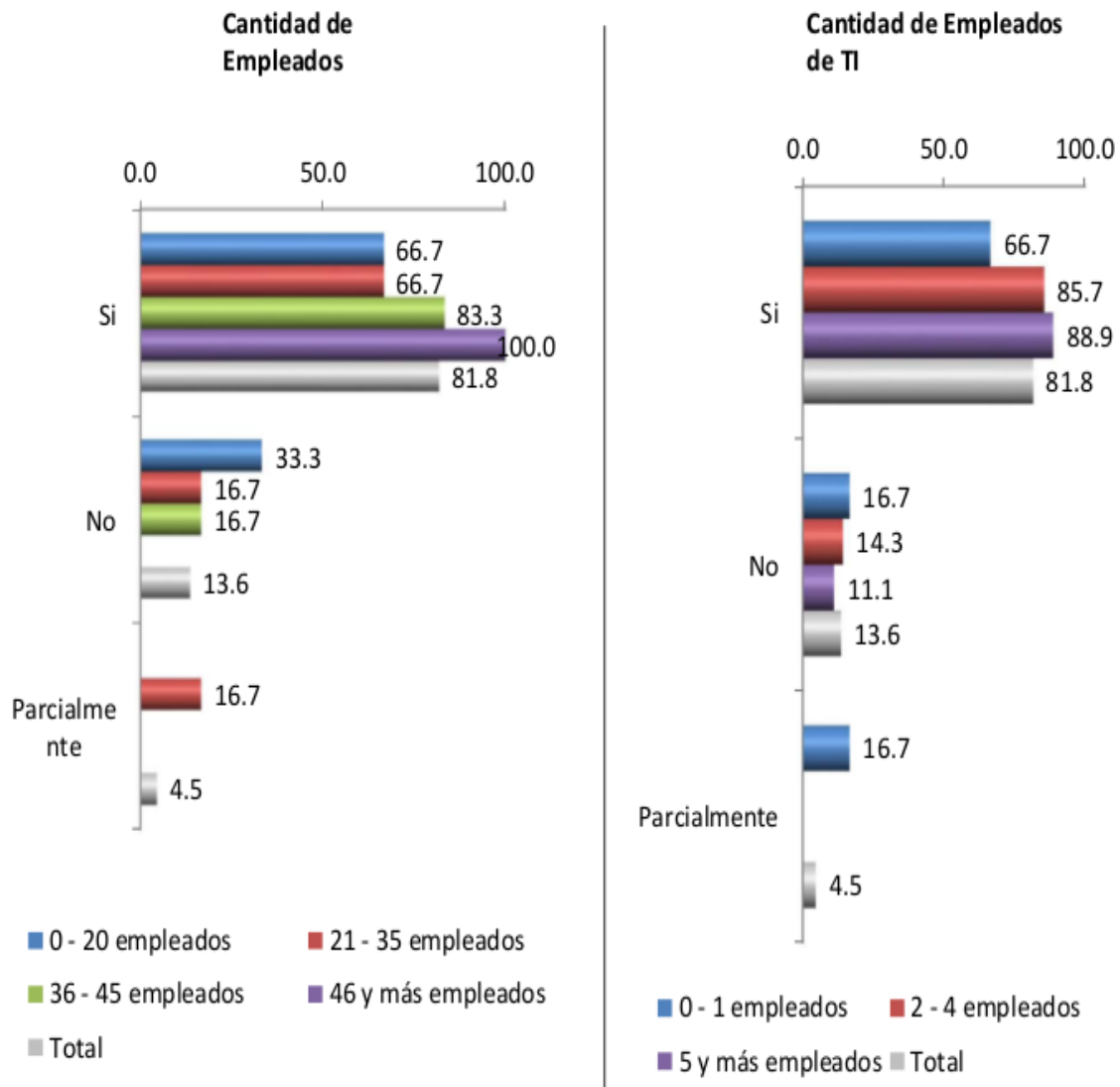


Cantidad de Empleados - Quienes en mayor medida manifiestan gestionar la cartera de proyectos de TI por los departamentos de la organización con la ayuda del departamento de TI son las empresas con más de 46 empleados.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan gestionar la cartera de proyectos de TI por los departamentos de la organización con la ayuda del departamento de TI son las empresas con 2 o más empleados de TI.

7.1.6 Realización de prácticas asociadas con el gobierno de las TI: Las necesidades de recursos de TI se identifican en consonancia con las prioridades de negocio según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 61. Realización de prácticas asociadas con el gobierno de las TI: Las necesidades de recursos de TI se identifican en consonancia con las prioridades de negocio según Cantidad de Empleados y Cantidad de Empleados de TI

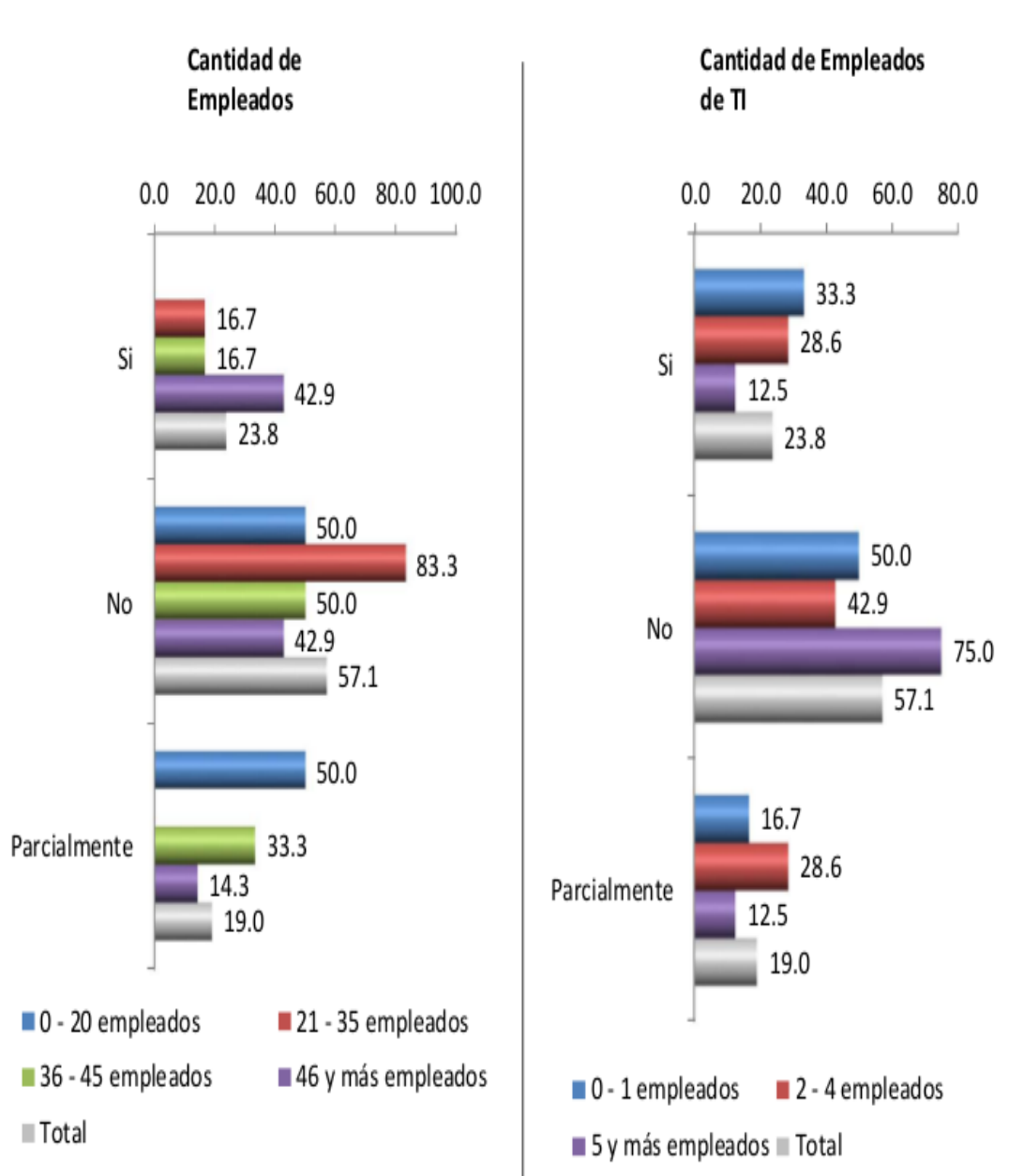


Cantidad de Empleados - Quienes en mayor medida manifiestan identificar las prioridades de negocio en consonancia con las necesidades de recursos de TI son las empresas con más de 36 empleados.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan identificar las prioridades de negocio en consonancia con las necesidades de recursos de TI son las empresas con 2 o más empleados de TI.

7.1.7 Realización de prácticas asociadas con el gobierno de las TI: Existe, de alguna manera, el Comité Estratégico de TI u órgano similar según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 62. Realización de prácticas asociadas con el gobierno de las TI: Existe, de alguna manera, el Comité Estratégico de TI u órgano similar según Cantidad de Empleados y Cantidad de Empleados de TI

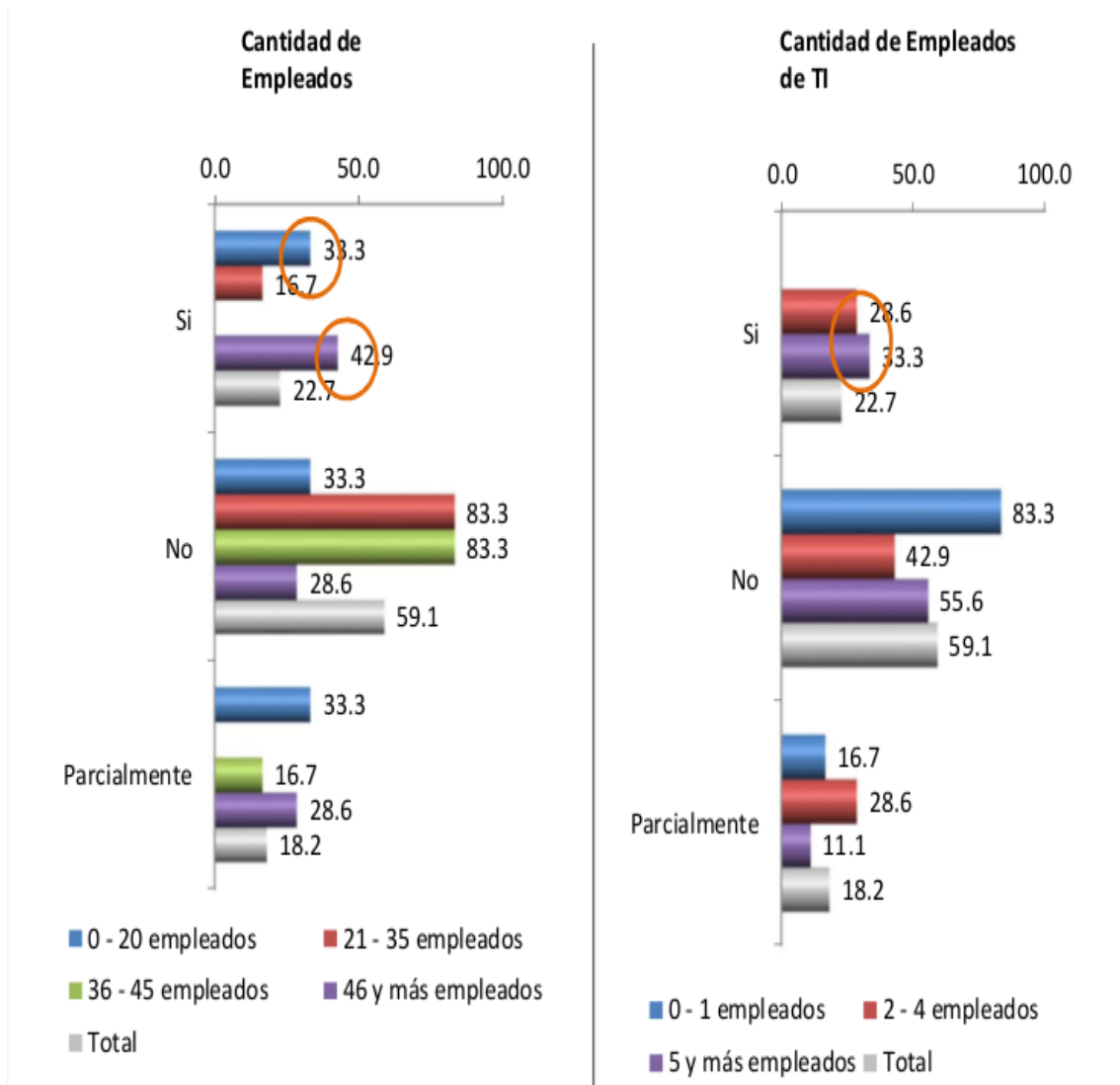


Cantidad de Empleados - Quienes en mayor medida manifiestan la existencia de un Comité Estratégico de TI u órgano similar son las empresas con más de 46 empleados.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan la existencia de un Comité Estratégico de TI u órgano similar son las empresas con menos de 5 empleados de TI.

7.1.8 Realización de prácticas asociadas con el gobierno de las TI: Existe un procedimiento estándar para la selección de inversiones de TI (Comité de Inversiones en TI) según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 63. Realización de prácticas asociadas con el gobierno de las TI: Existe un procedimiento estándar para la selección de inversiones de TI (Comité de Inversiones en TI) según Cantidad de Empleados y Cantidad de Empleados de TI

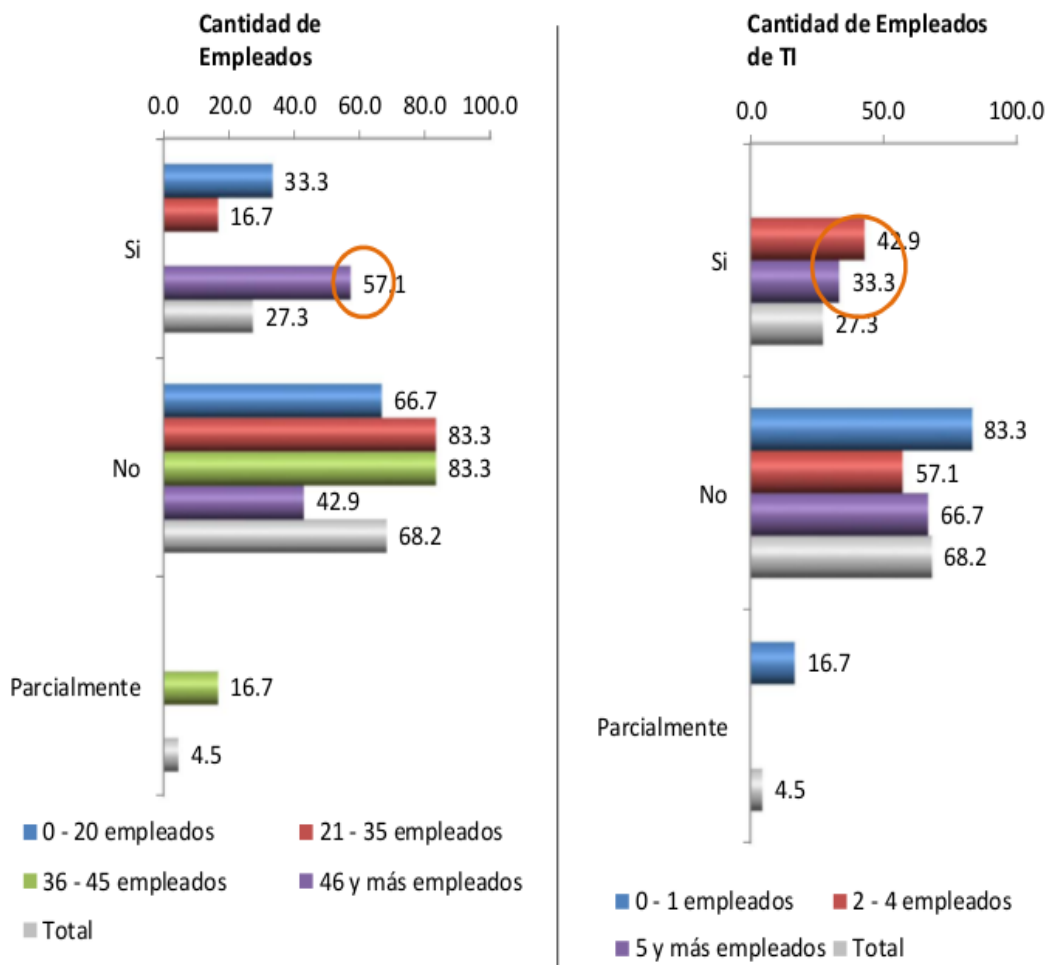


Cantidad de Empleados - Quienes en mayor medida manifiestan la existencia de un procedimiento estándar para la selección de inversiones en TI son las empresas con menos de 20 empleados y aquellas que tienen más de 46.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan la existencia de un procedimiento estándar para la selección de inversiones en TI son las empresas que tienen 2 o más empleados de TI.

7.1.9 Realización de prácticas asociadas con el gobierno de las TI: Existe un procedimiento estándar para determinar el valor (financiero y no financiero) y el riesgo en las inversiones de TI asociadas con el negocio según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 64. Realización de prácticas asociadas con el gobierno de las TI: Existe un procedimiento estándar para determinar el valor (financiero y no financiero) y el riesgo en las inversiones de TI asociadas con el negocio según Cantidad de Empleados y Cantidad de Empleados de TI

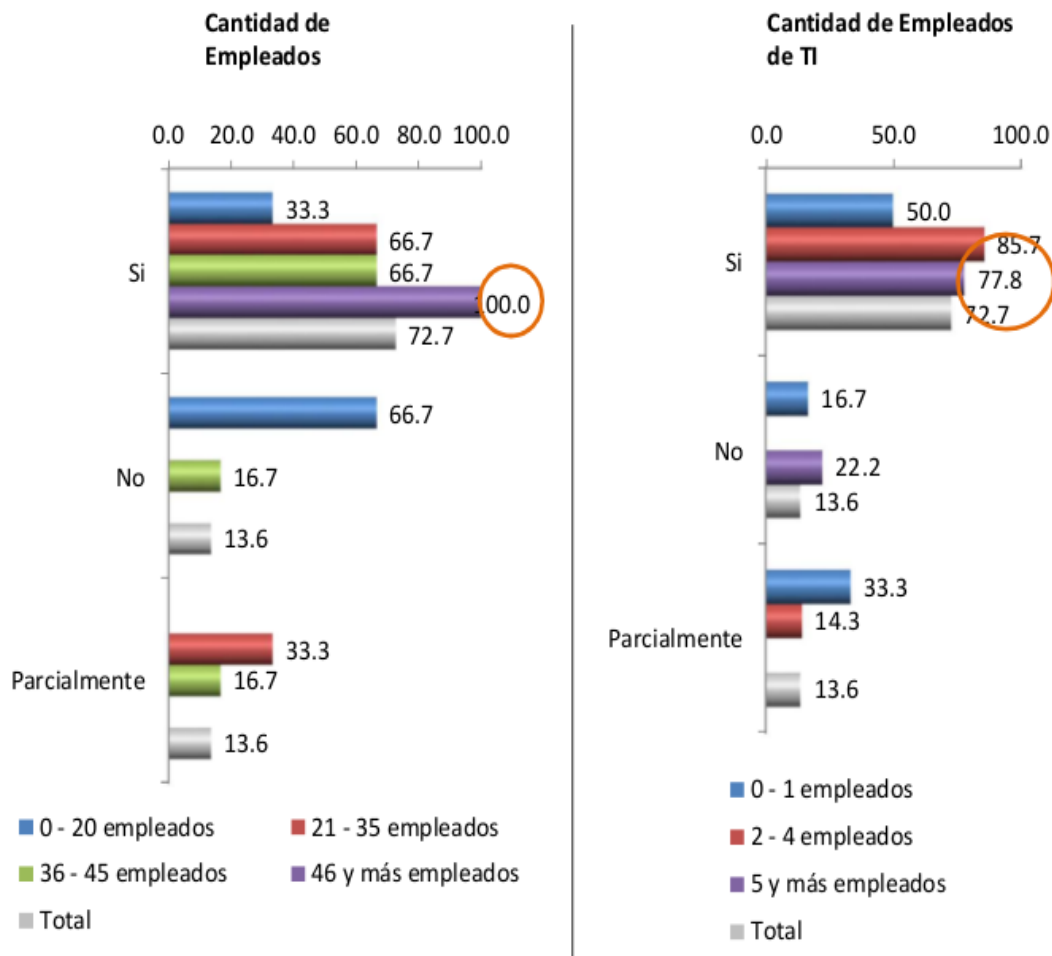


Cantidad de Empleados - Quienes en mayor medida manifiestan la existencia en su empresa de un procedimiento estándar para determinar el valor (financiero y no financiero) y el riesgo en las inversiones de TI asociadas con el negocio son las empresas con más de 46 empleados.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan la existencia en su empresa de un procedimiento estándar para determinar el valor (financiero y no financiero) y el riesgo en las inversiones de TI asociadas con el negocio son las empresas con 2 o más empleados de TI.

7.1.10 Realización de prácticas asociadas con el gobierno de las TI: El Gerente o Director General está informado de los riesgos más importantes asociados a las TI en la organización, y manda tomar las acciones adecuadas según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 65. Realización de prácticas asociadas con el gobierno de las TI: El Gerente o Director General está informado de los riesgos más importantes asociados a las TI en la organización, y manda tomar las acciones adecuadas según Cantidad de Empleados y Cantidad de Empleados de TI

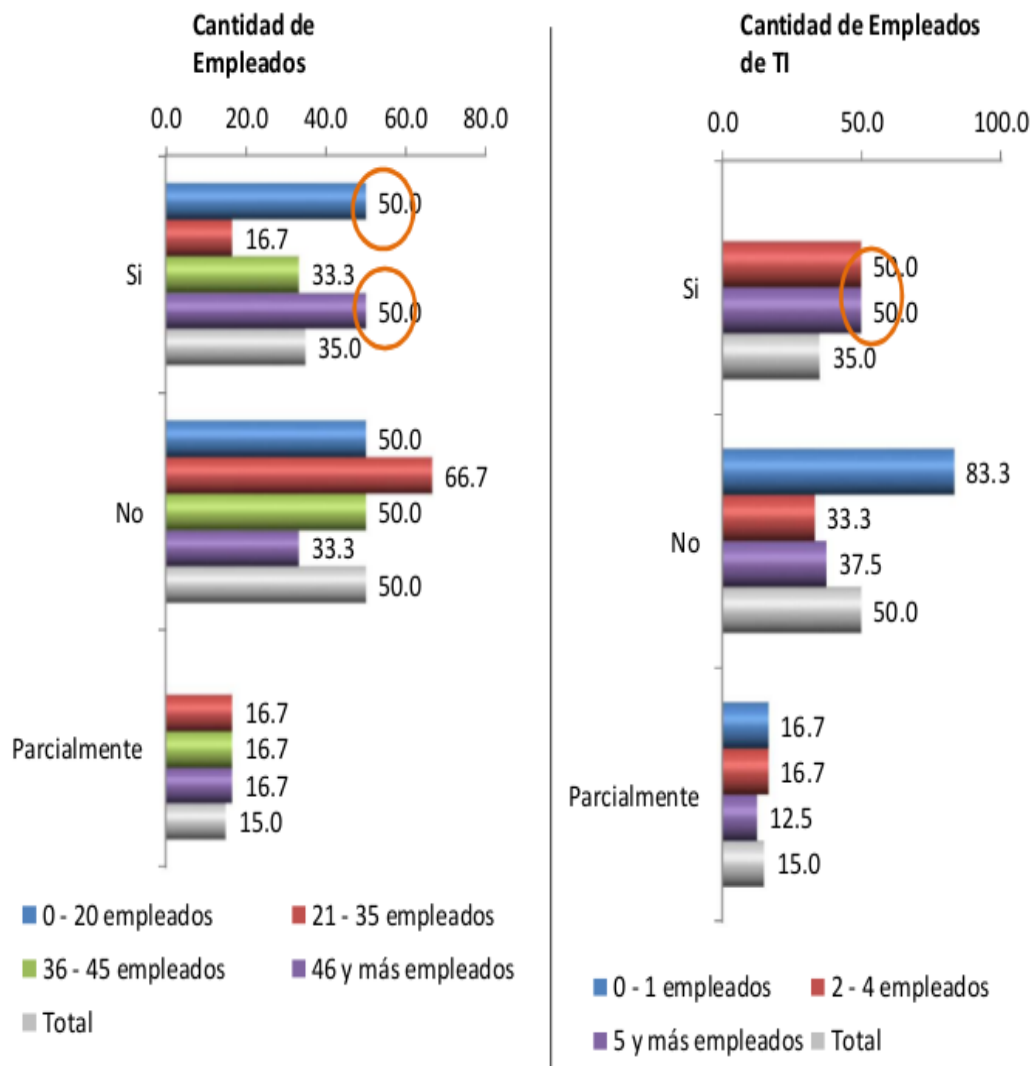


Cantidad de Empleados - Quienes en mayor medida manifiestan que el Gerente o Director general está informado de los riesgos más importantes asociados a las TI en la organización y manda tomar las acciones adecuadas son las empresas con más de 46 empleados.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan que el Gerente o Director general está informado de los riesgos más importantes asociados a las TI en la organización y manda tomar las acciones adecuadas son las empresas con 2 o más empleados de TI.

7.1.11 Realización de prácticas asociadas con el gobierno de las TI: Existe un cuadro de mando de TI que es utilizado por el negocio, y cubre aspectos asociados a la creación de valor según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 66. Realización de prácticas asociadas con el gobierno de las TI: Existe un cuadro de mando de TI que es utilizado por el negocio, y cubre aspectos asociados a la creación de valor según Cantidad de Empleados y Cantidad de Empleados de TI

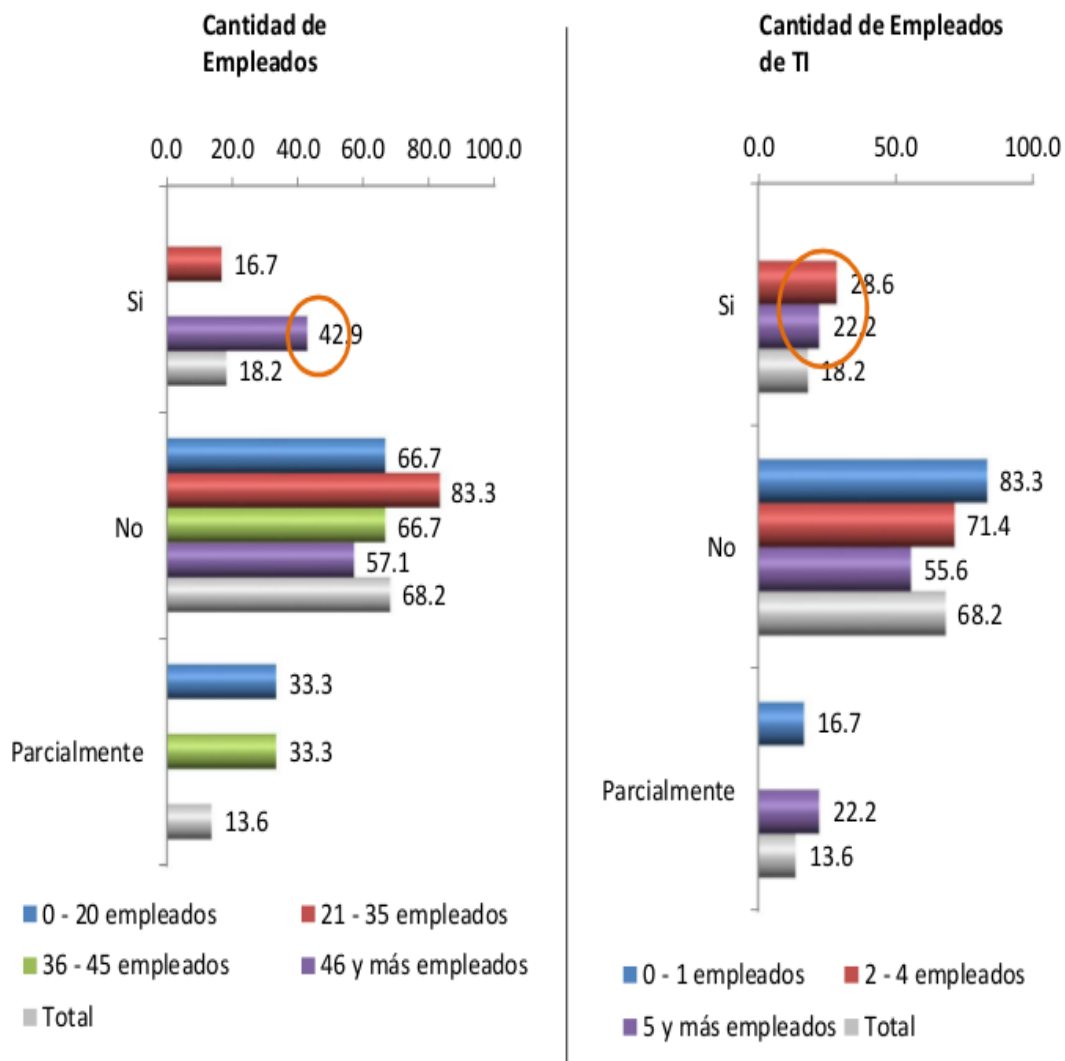


Cantidad de Empleados - Quienes en mayor medida manifiestan la existencia de un cuadro de mando de TI que es utilizado por el negocio y cubre aspectos asociados a la creación de valor son las empresas que tienen menos de 20 empleados y aquellas que cuentan con más de 46.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan la existencia de un cuadro de mando de TI que es utilizado por el negocio y cubre aspectos asociados a la creación de valor son las empresas que tienen 2 o más empleados de TI.

7.1.12 Realización de prácticas asociadas con el gobierno de las TI: Existe una supervisión central de la arquitectura de TI en la organización (Comité de Arquitectura de TI) según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 67. Realización de prácticas asociadas con el gobierno de las TI: Existe una supervisión central de la arquitectura de TI en la organización (Comité de Arquitectura de TI) según Cantidad de Empleados y Cantidad de Empleados de TI

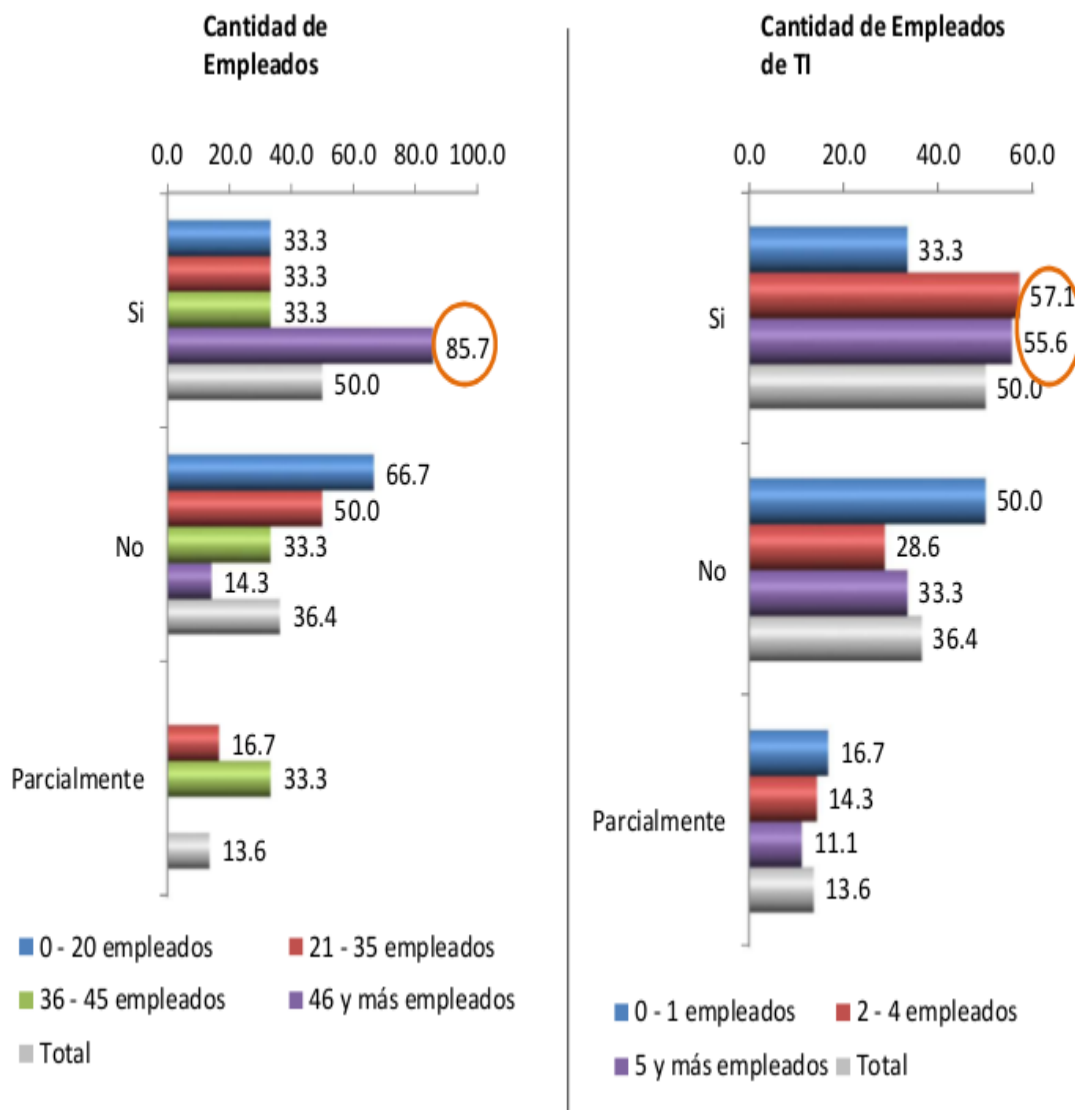


Cantidad de Empleados - Quienes en mayor medida manifiestan la existencia de una supervisión central de la arquitectura de TI en la organización son las empresas con más de 46 empleados.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan la existencia de una supervisión central de la arquitectura de TI en la organización son las empresas con 2 o más empleados de TI.

7.1.13 Realización de prácticas asociadas con el gobierno de las TI: Los procesos de TI se auditan regularmente para asegurar su efectividad y eficiencia según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 68. Realización de prácticas asociadas con el gobierno de las TI: Los procesos de TI se auditan regularmente para asegurar su efectividad y eficiencia según Cantidad de Empleados y Cantidad de Empleados de TI



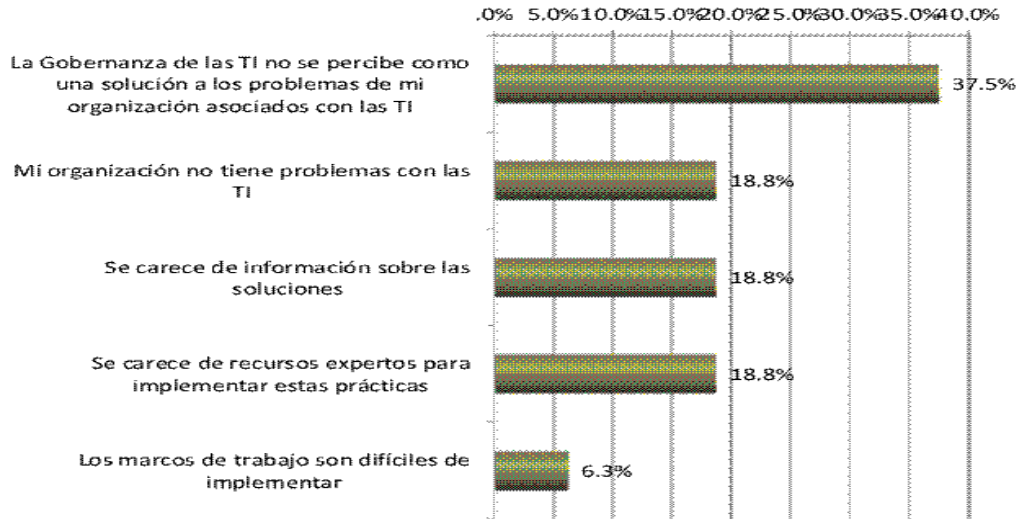
Cantidad de Empleados - Quienes en mayor medida manifiestan que los procesos de TI se auditan regularmente para asegurar su efectividad y eficiencia son las empresas con más de 46 empleados.

Cantidad de Empleados de TI - Quienes en mayor medida manifiestan que los procesos de TI se auditan regularmente para asegurar su efectividad y eficiencia son las empresas que cuentan con 2 o más empleados de TI.

7.2 Motivo de no implementación de las prácticas

Si no está considerando implementar prácticas en la pregunta anterior, indique el por qué

Grafica 69. Motivo de no implementación de prácticas



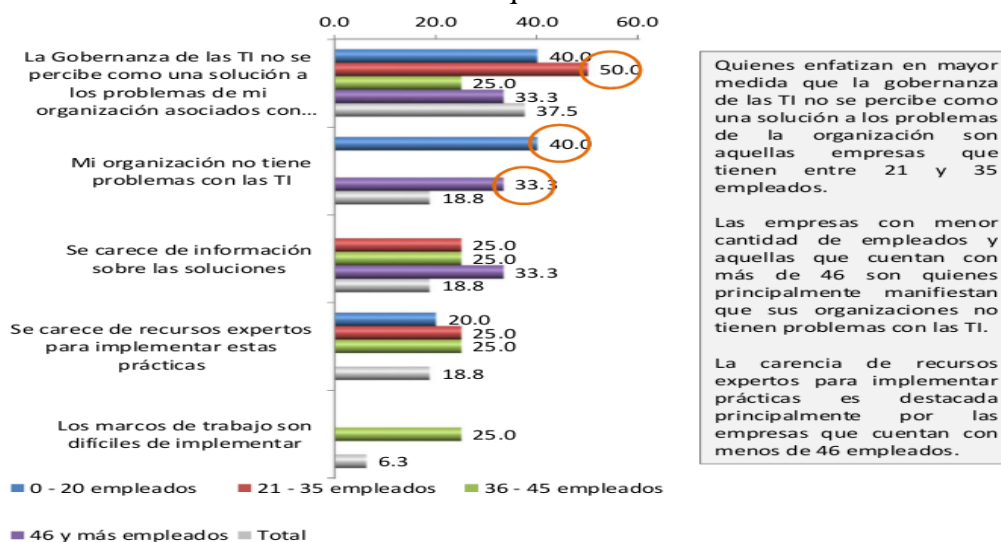
Para el 37% de las empresas consultadas, el principal motivo para no implementar las prácticas tiene que ver con que la gobernanza de las TI no se percibe como una solución a los problemas de la organización.

El 18,8% entiende que su organización no tiene problemas con las TI y quienes consideran como problema que se carece de información sobre las soluciones corresponden al 18,8% de los entrevistados.

Según el 18,8%, el principal problema refiere a la carencia de recursos expertos para la implementación de esas prácticas.

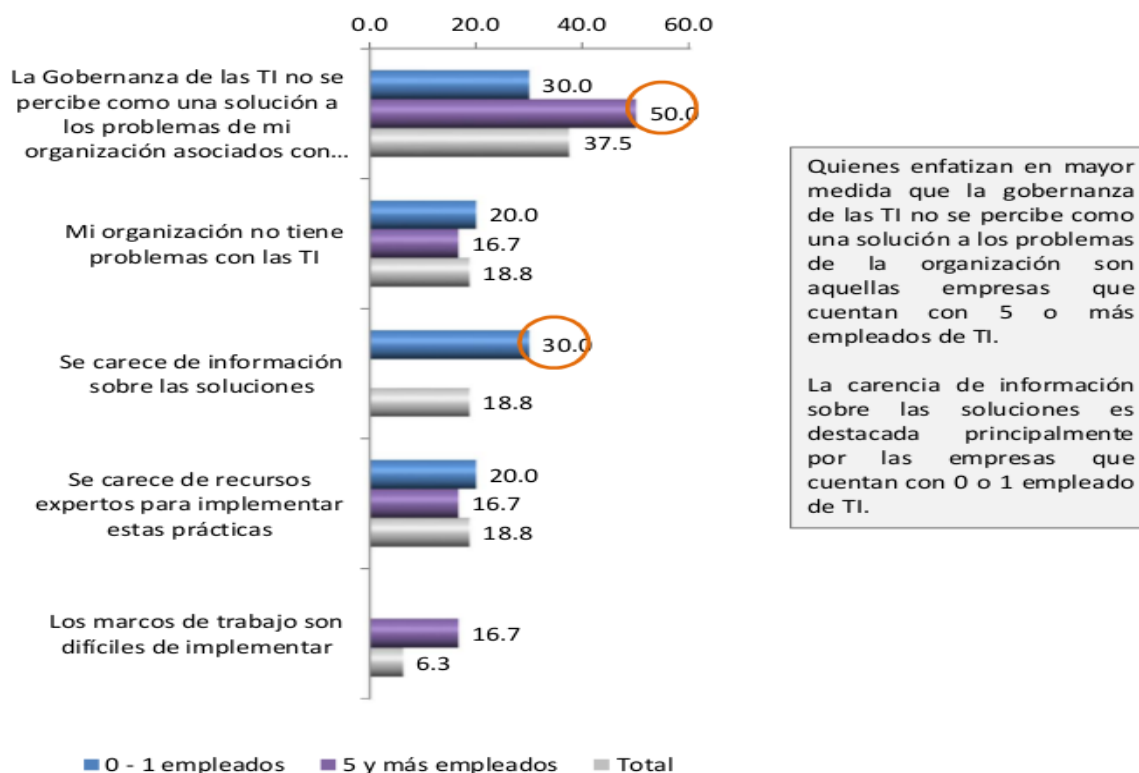
7.3 Motivo de no implementación de las prácticas según Cantidad de Empleados

Grafica 70. Si no está considerando implementar prácticas en la pregunta anterior, indique el por qué



7.4 Motivo de no implementación de las prácticas según Cantidad de Empleados de TI

Grafica 71. Si no está considerando implementar prácticas en la pregunta anterior, indique el por qué.



7.5 Implementación de alguna medida para mejorar en alguno de los siguientes aspectos

Figura 9. ¿Ha implementado o está en proceso de implementar alguna medida para mejorar en alguno de los siguientes aspectos?

Medida	% de casos
Entrega de valor de TI asociada a una mejor relación con los clientes	16,2%
Alineamiento entre la estrategia de TI y la estrategia global del negocio	14,3%
Gestión de recursos de TI (personas, sistemas, datos financieros, etc.)	14,3%
Entrega de valor de TI asociada a una reducción de costos	14,3%
Entrega de valor de TI asociada a un mayor liderazgo/innovación en productos/servicios	12,4%
Gestión activa del ROI (retorno de la inversión) de TI	10,5%
Gestión del riesgo de TI	9,5%
Medidas de rendimiento actual de TI	8,6%

7.6 Implementación de alguna medida para mejorar en alguno de los siguientes aspectos según Cantidad de Empleados

Figura 10. ¿Ha implementado o está en proceso de implementar alguna medida para mejorar en alguno de los siguientes aspectos?

	0 - 20 empleados	21 - 35 empleados	36 - 45 empleados	46 y más empleados	Total
Entrega de valor de TI asociada a una mejor relación con los clientes	12,5	14,7	20,0	16,3	16,2
Alineamiento entre la estrategia de TI y la estrategia global del negocio	12,5	11,8	15,0	16,3	14,3
Gestión de recursos de TI (personas, sistemas, datos financieros, etc)	12,5	11,8	20,0	14,0	14,3
Entrega de valor de TI asociada a una reducción de costos	12,5	14,7	15,0	14,0	14,3
Entrega de valor de TI asociada a un mayor liderazgo/innovación en productos/servicios	25,0	14,7	10,0	9,3	12,4

7.7 Implementación de alguna medida para mejorar en alguno de los siguientes aspectos según Cantidad de Empleados de TI

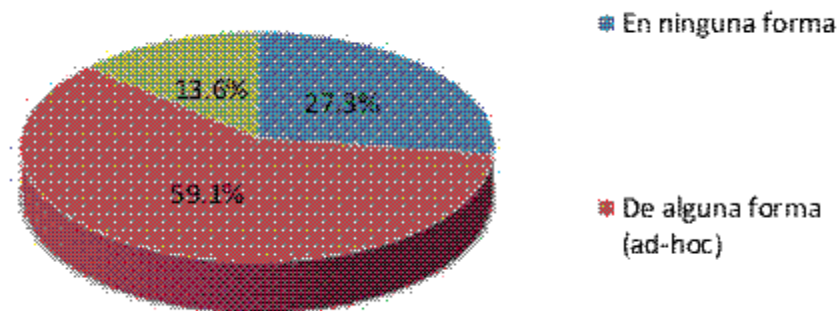
	0 - 1 empleados	2 - 4 empleados	5 y más empleados	Total
Entrega de valor de TI asociada a una mejor relación con los clientes	18,8	15,4	16,0	16,2
Alineamiento entre la estrategia de TI y la estrategia global del negocio	18,8	15,4	12,0	14,3
Gestión de recursos de TI (personas, sistemas, datos financieros, etc.)	18,8	12,8	14,0	14,3
Entrega de valor de TI asociada a una reducción de costos	12,5	12,8	16,0	14,3
Entrega de valor de TI asociada a un mayor liderazgo/innovación en productos/servicios	6,3	7,7	18,0	12,4
Gestión activa del ROI (retorno de la inversión) de TI	12,5	12,8	8,0	10,5

Figura 11. ¿Ha implementado o está en proceso de implementar alguna medida para mejorar en alguno de los siguientes aspectos?

7.8 Medición del progreso en la Gobernanza de TI

¿En qué grado mide su progreso en la Gobernanza de TI?

Grafica 72. Medición del progreso en la Gobernanza

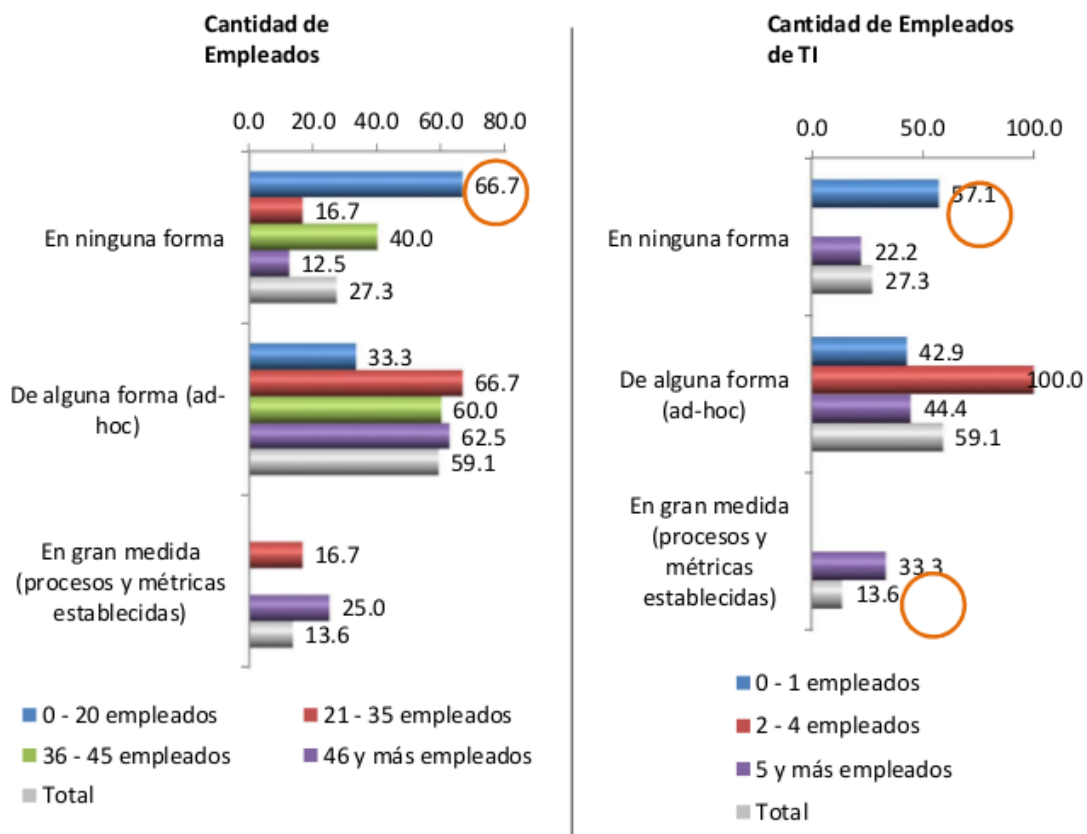


Casi el 60% de los entrevistados, mide de alguna forma (ad-hoc) su progreso en la gobernanza de TI.

El 27% explica que no mide su progreso y el restante 13% menciona que mide en gran medida su progreso en la gobernanza de TI.

7.9 Medición del progreso en la Gobernanza de TI según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 73. ¿En qué grado mide su progreso en la Gobernanza de TI?



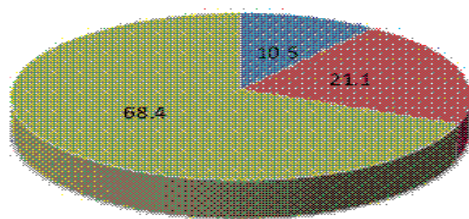
Cantidad de Empleados - Las empresas con menos de 20 empleados son las que en mayor medida no miden de ninguna forma su progreso en la gobernanza de TI. Quienes manifiestan realizar mediciones «en gran medida (mediante procesos y métricas establecidas)», son mayormente las empresas con más de 46 empleados y aquellas que tienen entre 21 y 35 empleados.

Cantidad de Empleados de TI - Las empresas con 0 o 1 empleados de TI son las que en mayor medida no miden en ninguna forma el progreso de la gobernanza de TI. Solo empresas que tienen 5 o más empleados manifiestan realizar mediciones «en gran medida».

7.10 Prácticas de Gobernanza de TI como mejora de la eficiencia de los costos de TI para el negocio

¿Cree que las prácticas de Gobernanza de TI han permitido mejorar la eficiencia de los costos de TI para el negocio?

Grafica 74. Práctica como mejora de eficiencia

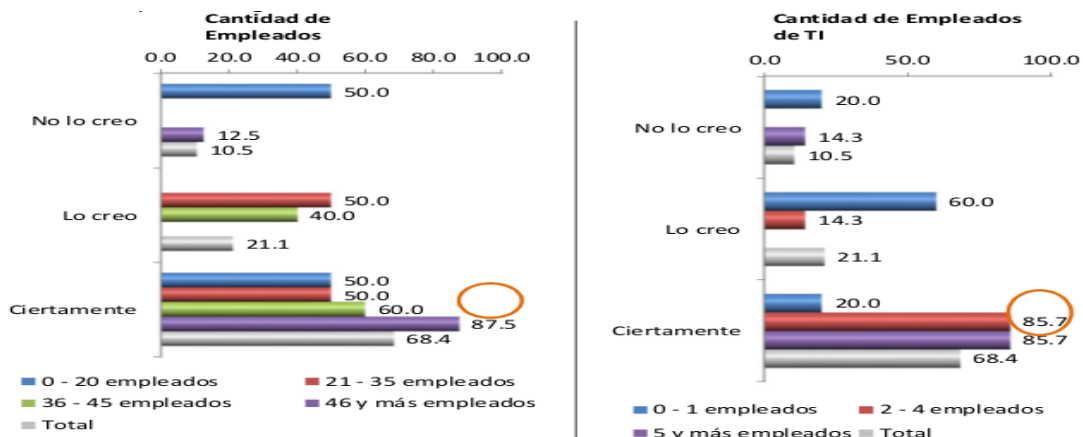


El 68% de los entrevistados, entiende que las prácticas de Gobernanza de TI ciertamente mejoran la eficiencia de los costos para el negocio. El 21% cree que sirven para mejorar y el 10% entiende que estas prácticas no mejoran la eficiencia de los costos.

■ No lo creo ■ Lo creo ■ Ciertamente

7.11 Prácticas de Gobernanza de TI como mejora de la eficiencia de los costos de TI para el negocio según Cantidad de Empleados y Cantidad de Empleados de TI

Grafica 75. ¿Cree que las prácticas de Gobernanza de TI han permitido mejorar la eficiencia de los costos de TI para el negocio?



Cantidad de Empleados - Quienes manifiestan en mayor medida que las prácticas de gobernanza de TI han permitido mejorar la eficiencia de los costos de TI para el negocio son las empresas con más de 46 empleados.

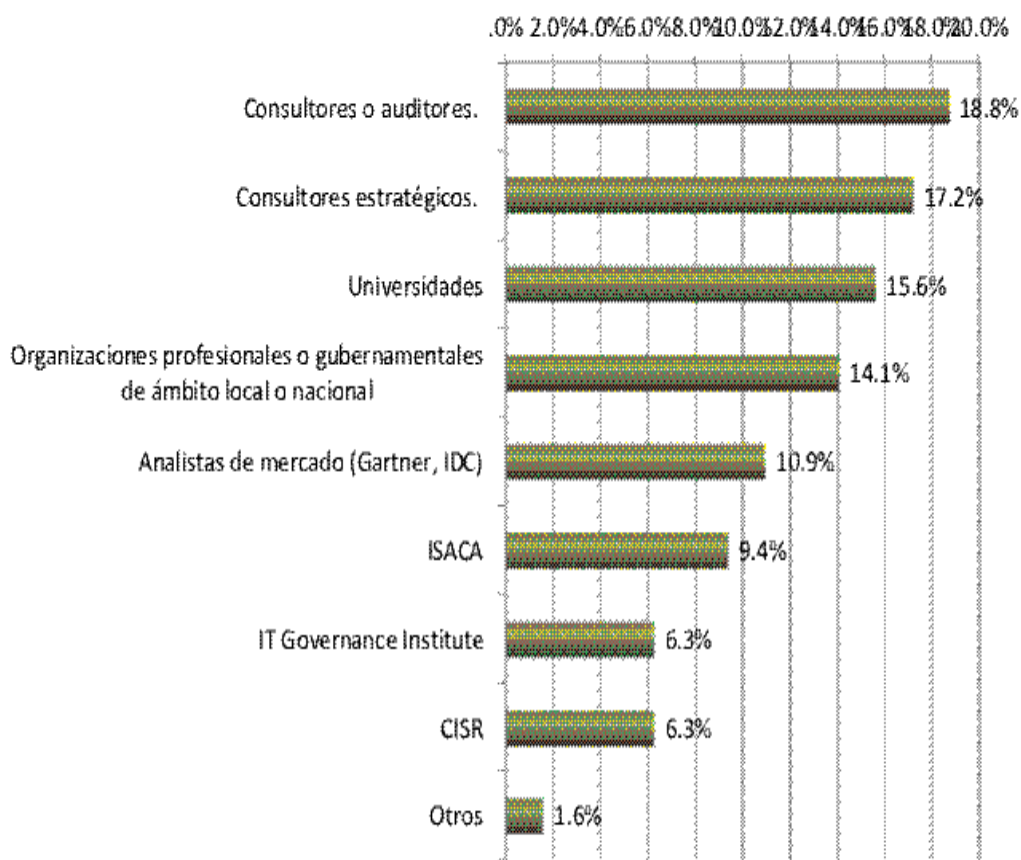
Cantidad de Empleados de TI – Quienes manifiestan en mayor medida que las prácticas de gobernanza de TI han permitido mejorar la eficiencia de los costos de TI para el negocio son las empresas que cuentan con 2 o más empleados de TI.

8. CONOCIMIENTO DE HERRAMIENTAS Y ORGANIZACIONES DE GOBERNANZA DE TI

8.1 Organizaciones que proporcionan o implementan soluciones a problemas de Gobernanza de TI

¿Cuál de las siguientes organizaciones conoce que proporcionan o implementan soluciones a los problemas de Gobernanza de TI?

Grafica 76. Organizaciones que proporcionan soluciones a problemas de gobernanza de TI



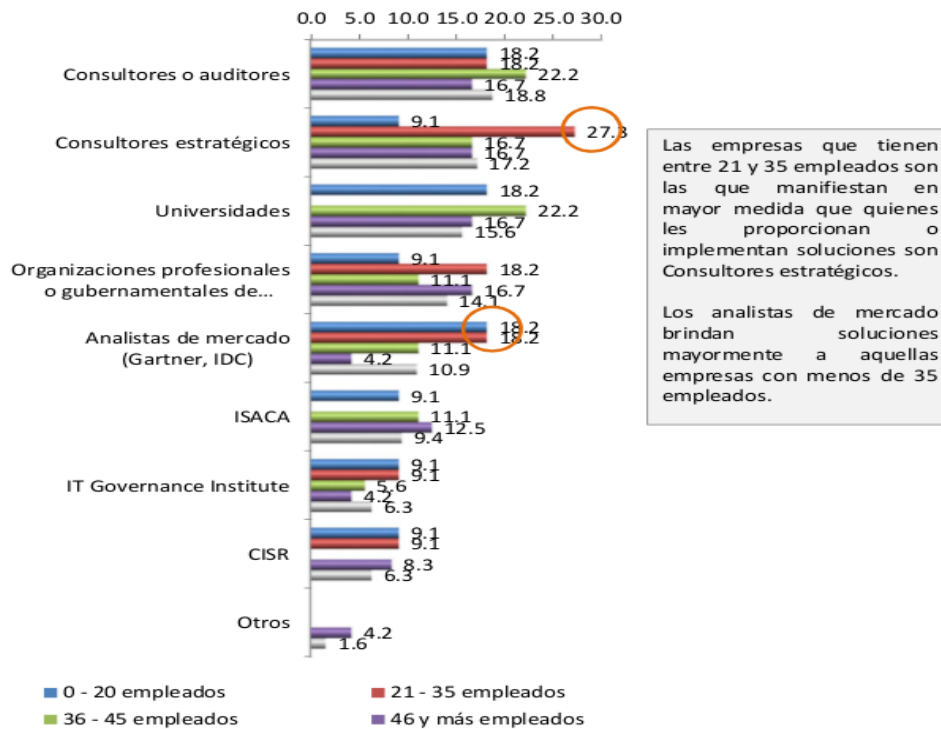
El 18% de las empresas, explica que son los consultores o auditores los que proporcionan las soluciones de gobernanza de TI.

Para el 17% son los consultores estratégicos los que se encargan de dar estas soluciones.

Según el 15% de los entrevistados, son las universidades quienes implementan estas soluciones y para el 14% de las empresas consultadas, son las organizaciones profesionales o gubernamentales de ámbito local o nacional quienes solucionan los problemas de gobernanza de TI.

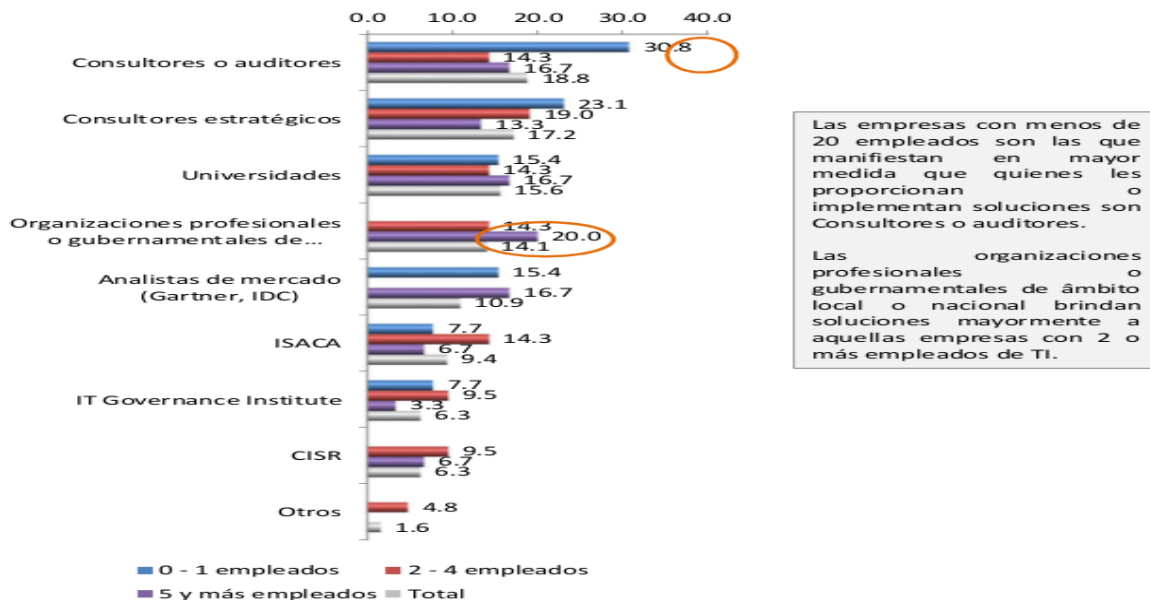
8.2 Organizaciones que proporcionan o implementan soluciones a problemas de Gobernanza de TI según Cantidad de Empleados

Grafica 77. ¿Cuál de las siguientes organizaciones conoce que proporcionan o implementan soluciones a los problemas de Gobernanza de TI?



8.3 Organizaciones que proporcionan o implementan soluciones a problemas de Gobernanza de TI según Cantidad de Empleados de TI

Grafica 78. ¿Cuál de las siguientes organizaciones conoce que proporcionan o implementan soluciones a los problemas de Gobernanza de TI?



Anexo VII - Guía de relevamiento

La planilla siguiente, es una herramienta para medir la madurez de la empresa, la cual brinda una referencia sobre la aplicación del modelo, para cada nivel respecto a cada indicador. Luego de aplicar el modelo en una empresa, se podrá contrastar con los niveles presentes en esta planilla y se podrá gráfica y rápidamente determinar a qué nivel se asemeja. Sirve así de guía de relevamiento del modelo de madurez.

Dominio		Proceso / Actividad	Indicador	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Proceso Gobierno del Riesgo	RG						
	RG 1.1	Desarrollar en una empresa el marco específico de gestión de riesgos de TI	1. Porcentaje de variables de negocio para las cuales se ha identificado y registrado los puntos de TI que pueden aportar valor al negocio, para los cuales existe un análisis de tolerancia al riesgo. Registro de variables con tolerancia al riesgo en los rangos: 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	No Existe	20-40%	40-60%	60-100%
			2. Existencia de mapas de conocimiento que vinculan los eventos de TI identificados.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RG 1.2	Proponer los umbrales de tolerancia de riesgos de TI	1. Porcentaje de procesos de negocio que cuentan con medidas de riesgo y niveles de tolerancia asociados. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	0-20%	20-40%	40-60%	60-100%

			2. Existencia de recursos humanos capacitados para la definición de umbrales de tolerancia de riesgos de TI. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	0-20%	20-40%	40-60%	60-100%
	RG 1.3	Aprobar la tolerancia al riesgo	1. Existencia de mapas de conocimiento y base de conocimiento de todas las áreas de la empresa con umbrales de riesgo por área de negocio.	No Existe	Existe	Existe y se desarrolla	Uso y Mejora
	RG 1.4	Alinear la política de riesgos de TI	1. Existencia de base de conocimiento de la organización con apetito al riesgo y tolerancia de cada área de negocio.	No Existe	Existe	Existe y se desarrolla	Uso y Mejora
			2. Nro de horas de reunión de grupos de expertos por cada área sobre el número de áreas de negocio de la empresa, dedicados a la definición del apetito y tolerancia al riesgo de cada área respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%

	RG 1.5	Promover los riesgos de TI – cultura consciente	1. Horas dedicadas en cursos sobre nro de personas capacitadas en gestión del riesgo para cada área de negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			2. Existencia de base de conocimientos con registro de acciones y buenas prácticas en gestión del riesgo de cada área de negocio.	No Existe	Existe	Existe y se desarrolla	Uso y Mejora
			3. Existencia del rol CKO dedicado a la comunicación de la política de gestión del riesgo en la organización.	No Aplica	Existe	Existe y comunica activamente	Comunica en toda la organización
			4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	No Existe	Existe	Existen políticas y normas	Exige promoción de políticas y normas
	RG 1.6	Promover una comunicación efectiva de los riesgos de TI	1. Existencia de un plan de comunicación de riesgos	No Aplica	Existe	Existe y se actualiza	
			2. Existencia de una base de conocimiento organizacional accesible por responsables y directores con información sobre amenazas e impacto de riesgos por área.	No Existe	Existe	Existe y esta disponible	

			3. Nro de amenazas por área de negocio registradas en la base de conocimiento. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	0-20%	20-40%	40-60%	60-100%
			4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	No Existe	Existe	Existen políticas y normas	
	RG 2.1	Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes.	No Aplica	Existe	Existe y desarrolla	Uso y Mejora
			2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	No Aplica	20-40%	40-60%	60-100%

	RG 2.2	Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial	1. Horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			2. Horas de reuniones dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	No Existe	20-40%	40-60%	60-100%
	RG 2.3	Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa	1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			3. Porcentaje de recursos de la empresa capacitados o que asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	0-20%	20-40%	40-60%	60-100%
	RG 2.4	Proporcionar recursos adecuados para la gestión de riesgos	1. Nro de horas en capacitación al personal de cada área en gestión del riesgo sobre total de recursos humanos del área.	No Existe	5-10%	10-15%	15-20%
			2. Existencia de una base de conocimiento de la organización y mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RG 2.5	Garantizar el aseguramiento independiente sobre la gestión de riesgos	1. Existe una base de conocimiento con el registro del apetito al riesgo y tolerancia que permite la gestión del riesgo por parte del director de TI y director general.	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			2. Existencia de mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			3. Horas en capacitación de recursos humanos asegurando su independencia en la gestión de riesgos respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
	RG 3.1	Ganancia de la gestión de compra para el enfoque de análisis de riesgos	1. Existe una base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			3. Horas de capacitación o reuniones que permitan interpretar los informes de análisis de riesgo y brechas existentes con el riesgo empresarial, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%

			4. Horas de capacitación en concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos de la empresa, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Existe	5-10%	10-15%	15-20%
	RG 3.2	Aprobar el análisis de riesgos de TI	1. Existe una base de conocimiento única para las distintas áreas de la empresa accesible a todos los directores de área que permite registrar, transmitir y usar dicho conocimiento.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			2. Nro de horas en capacitación y reuniones para la formación de los directores de área en la cultura de gestión del riesgo a través de la gestión del conocimiento respecto al total de horas de los directores. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Existe	5-10%	10-15%	15-20%
	RG 3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			3. Horas de capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Existe	5-10%	10-15%	15-20%
	RG 3.4	Aceptar los riesgos de TI	1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			<p>3. Horas de capacitación en formación al personal sobre aceptación y gestión del riesgo de TI para el negocio de cada área de la empresa respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	No Existe	5-10%	10-15%	15-20%
	RG 3.5	Priorizar actividades de respuesta de riesgos de TI	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa disponible para el director general y director de TI, que permita registrar métricas para el seguimiento del cumplimiento de las actividades de TI, así como priorización de las mismas, con información sobre el apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			<p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			3. Horas de capacitación y formación al director general y de TI sobre seguimiento y planificación de riesgos en TI respecto al total de horas de los directores general y de TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Existe	5-10%	10-15%	15-20%
Proceso Evaluación del Riesgo	RE						
	RE 1.1	Establecer y mantener un modelo para la recolección de datos	1. Existe apoyo explícito de la dirección para la concreción de la recopilación de datos para la formación de un repositorio único de conocimiento, así como en la culturización en gestión del conocimiento en la empresa.	No Existe	Existe	Existen políticas y normas	Exige promoción de políticas y normas
			2. Existe una estrategia de adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			3. Existe una implementación para la adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			4. Horas de capacitación y formación realizadas con el personal de la empresa respecto a la recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento en la organización, respecto al total de horas del personal. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
	RE 1.2	Recopilar datos sobre el entorno externo	1. Horas de reuniones de benchmarking, charlas informales y con expertos, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
	RE 1.3	Recopilar datos sobre eventos de riesgo	1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%

	RE 1.4	Identificar factores de riesgo	<p>1. Horas de reuniones de charlas con expertos, coaching, comunidades de práctica realizadas por directivos de TI y de las restantes áreas de la empresa, aplicadas para la identificación de riesgos, asociados a proyectos, programas, servicios existentes y futuros, etc. que pueden generar eventos de riesgo, respecto al total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
			<p>2. Existencia de una base de conocimiento organizacional donde se integra información sobre proyectos, programas, servicios e incidentes.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RE 2.1	Definir Alcance del Análisis de Riesgo	<p>1. Horas de capacitación y formación al personal responsable de la gestión del riesgo y del negocio de la empresa, en cuanto a gestión y evaluación del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%

			<p>2. Horas de reuniones de charlas con expertos, benchmarking, realizadas con el personal responsable de la gestión del riesgo y el negocio sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
	RE 2.2	Estimación de riesgos en TI	<p>1. Horas de capacitación y formación a los responsables del riesgo y de negocio de la empresa, sobre análisis de información de riesgo (factores, frecuencia, magnitud y tolerancia al riesgo) para la estimación y definición de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
			<p>2. Existencia de un CMS disponible para el análisis en la estimación de riesgos.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			3. Horas de reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos en el CMS de la empresa.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RE 2.3	Identificar las opciones de respuesta de riesgo	1. Horas de capacitación y formación a los directivos y responsables del riesgo sobre identificación de respuestas de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			2. Existencia de un CMS disponible para la consulta y actualización de respuestas de riesgo.	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
			<p>4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas de riesgos en el CMS de la empresa.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RE 2.4	Realizar una revisión por pares de los resultados de análisis de riesgos de TI	<p>1. Horas de capacitación y formación a los responsables del riesgo sobre la aplicación de técnicas para el análisis de riesgos de TI respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
			<p>2. Existencia de un CMS disponible para la actualización de la información sobre riesgos de TI en la empresa.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			3. Horas de reuniones de charlas con expertos, charlas formales e informales, coaching en asignación de recursos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			4. Aplicación de sistemas expertos en la resolución de la asignación de recursos.	Ocasional	Aplica	Aplica activamente	Mejora el uso
	RE 3.1	Mapa de recursos de TI para procesos de negocio	1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			2. Horas de capacitación y formación a los responsables del riesgo en la empresa, sobre uso y análisis de mapas de conocimiento respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
	RE 3.2	Determinar la criticidad de negocios de los recursos de TI	1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			<p>2. Horas de capacitación y formación a los responsables de la gestión de los recursos en las distintas áreas de la empresa, sobre la determinación de criticidad de los recursos según los requerimientos de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
			<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales para la definición de la criticidad de los recursos de TI en cada área respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
			<p>4. Existencia de un CMS con información sobre riesgos, recursos y su criticidad.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RE 3.3	Entender las capacidades de TI	<p>1. Horas de capacitación y formación de los responsables de TI y responsables de cada área, para la evaluación de las capacidades disponibles y análisis de situación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%

			2. Existe plan de capacitación de los responsables de cada área y de TI, sobre gestión del riesgo de TI.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			4. Existencia de un CMS con información sobre las capacidades y requerimientos en TI de la empresa.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			5. Horas de reuniones de charlas formales e informales, consultas a expertos, sobre análisis de las capacidades existentes en TI y sus requerimientos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
	RE 3.4	Actualización de los componentes del escenario de riesgos de TI	1. Horas de capacitación y formación de los responsables de negocio, riesgo y TI, para la evaluación de escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%

			2. Existencia de un CMS con información sobre riesgos y distintos escenarios de riesgo.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			3. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre análisis de distintos escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
	RE 3.5	Mantener los riesgos de TI y mapa de registro de riesgos de TI	1. Horas de capacitación y formación de los responsables de negocio y TI, para la actualización de riesgos de TI y definición de perfil de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			2. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre definición de perfil de riesgo de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%

			3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RE 3.6	Diseñar y comunicar los indicadores de riesgo de TI	1. Existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo en TI en la empresa.	No Existe	Existe	Existen políticas y normas	Facilita y exige diseño y comunicación de indicadores
			2. Horas de reuniones de charlas formales y consultas a expertos sobre difusión de indicadores de riesgo de la empresa respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			3. Existencia de conocimiento actualizado sobre buenas prácticas en difusión de indicadores en la base de conocimiento de la empresa.	No Existe	Existe	Existe y se actualiza	Uso y Mejora
Proceso Respuesta del Riesgo	RR						

	RR 1.1	Informe de los resultados de análisis de riesgos de TI	1. Horas de reuniones de charlas formales, consultas a expertos, coaching, mentoring sobre gestión de la comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			2. Horas de capacitación y formación sobre técnicas y herramientas de comunicación y coordinación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			3. Existe un CMS a nivel de la organización que permite adquirir el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, por parte de los responsables de negocio, riesgo y directores.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RR 1.2	Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	1. Horas de reuniones de charlas formales e informales, consultas a expertos, coaching, mentoring sobre generación de informes y comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%

			2. Existe un CMS a nivel de la organización que permite la distribución de la información estratégica resultado de la gestión de riesgos.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			3. Existencia de conocimiento actualizado en el CMS sobre lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RR 1.3	Interpretar resultados de la evaluación independiente de TI	1. Existencia de conocimiento actualizado en el CMS para el análisis de acciones correctivas e identificación de oportunidades de mejora.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			2. Horas de capacitación y formación de recursos humanos de la empresa en el análisis del conocimiento del CMS para la generación de planes de acción correctiva respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			3. Existencia de un plan de acción correctiva	No Aplica	Existe	Existe y desarrolla	Uso y Mejora

			<p>4. Horas de reuniones de charlas formales e informales, contacto personal, mentoring sobre el análisis de acciones correctivas y mejoras en la gestión del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
	RR 1.4	Identificar TI – Oportunidades relacionadas	<p>1. Horas de capacitación y formación de recursos humanos responsables de TI y del negocio de la empresa en el análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	No Aplica	5-10%	10-15%	15-20%
			<p>2. Horas de reuniones de charlas con expertos, coaching, benchmarking sobre optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	No Existe	5-10%	10-15%	15-20%
	RR 2.1	Controles del inventario	<p>1. Existencia de conocimiento actualizado en el CMS para el control de inventario de riesgos.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			<p>2. Horas de capacitación y formación de recursos humanos de la empresa en el control de inventarios de riesgo y clasificación de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
			<p>3. Horas de reuniones de charlas formales e informales, coaching y mentoring sobre control del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
	RR 2.2	Supervisar la alineación operacional de los umbrales de tolerancia al riesgo	<p>1. Existe apoyo explícito de la dirección en la definición de indicadores de riesgo y definición de umbrales de tolerancia al riesgo.</p>	No Existe	Existe	Aplica activamente	Facilita y exige definición de indicadores y umbrales
			<p>2. Existe un CMS de la organización con riesgos, tolerancia al riesgo y umbrales, disponible para la supervisión de la alineación operacional de los umbrales a la tolerancia al riesgo.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora

			3. Existen reuniones de charlas y grupos de expertos para el logro de la aceptación de indicadores por parte de las áreas operativas y dirección.	No Existe	Existe	10-15%	15-20%
			4. Horas de capacitación a la dirección en la definición de umbrales de tolerancia al riesgo y supervisión respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Existe	5-10%	10-15%	15-20%
	RR 2.3	Responder a la exposición al riesgo descubierto y la oportunidad	1. Existencia de conocimiento actualizado en el CMS para la respuesta al riesgo.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			2. Horas de reuniones de charlas formales e informales, coaching, mentoring sobre respuestas al riesgo descubierto y oportunidades respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			3. Existencia de un mapa de conocimiento que facilite el acceso y distribución de los riesgos descubiertos y oportunidades.	No Existe	Existe	Existe y desarrolla	Uso y Mejora

	RR 2.4	Implementar los controles	1. Existe un CMS actualizado con el conocimiento sobre controles de riesgo.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			2. Horas de reuniones de coaching, mentoring, charlas formales e informales, sobre implementación de controles respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
			3. Existencia de un mapa de conocimientos actualizado que cuenta con la distribución del riesgo y controles existentes en la organización.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			4. Horas de capacitación y formación en la implementación de controles y uso de mapas de conocimiento para el mismo respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Existe	5-10%	10-15%	15-20%
	RR 2.5	Informe del progreso del plan de acción de riesgos de TI	1. Horas de capacitación al personal de TI y responsables del riesgo, en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Aplica	5-10%	10-15%	15-20%

			2. Horas de reuniones de charlas, grupos de expertos, benchmarking en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Aplica	5-10%	10-15%	15-20%
			3. Horas de reuniones destinadas a la comunicación sobre el progreso del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Aplica	5-10%	10-15%	15-20%
	RR 3.1	Mantener los planes de respuesta a incidentes	1. Existe un CMS actualizado de respuestas a incidentes, accesible a los responsables de TI y gestión del riesgo.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			2. Horas de reuniones en charlas, grupos de expertos sobre comunicación y gestión de planes de respuesta respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
	RR 3.2	Supervisión de riesgos de TI	1. Horas de capacitación a responsables del riesgo y auditores sobre supervisión de riesgo de TI respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Existe	5-10%	10-15%	15-20%

			2. Existencia de un CMS sobre riesgos y límites de la organización accesible a los responsables del riesgo y auditores.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
			3. Horas de reuniones con grupos de expertos, charlas formales e informales sobre mejora en los riesgos de TI en base a los riesgos y límites tolerados respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	0-5%	5-10%	10-15%	15-20%
	RR 3.3	Iniciar planes de respuesta a incidentes	1. Horas de capacitación y formación de responsables de la gestión y el riesgo de la empresa, en el logro de las mejores respuestas de cada incidente y el uso del CMS de la organización para ello respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No Existe	5-10%	10-15%	15-20%

			<p>2. Horas de reuniones en charlas formales e informales y benchmarking para lograr las mejores respuestas a incidentes y correcta distribución del conocimiento a los interesados respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	0-5%	5-10%	10-15%	15-20%
			<p>3. Existencia de una base de conocimiento actualizada con categorías de hechos y respuestas.</p>	No Existe	Existe	Existe y desarrolla	Uso y Mejora
	RR 3.4	Comunicar las lecciones aprendidas de eventos de riesgo	<p>1. Horas de capacitación y formación de responsables de TI y del riesgo de la empresa, en la identificación de las causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	No Existe	5-10%	10-15%	15-20%
			<p>2. Horas de capacitación en charlas, grupos de expertos y benchmarking sobre identificación de causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	No Existe	5-10%	10-15%	15-20%

			3. Existencia de un CMS actualizado con datos históricos y recientes de acontecimientos adversos y pérdidas.	No Existe	Existe	Existe y desarrolla	Uso y Mejora
--	--	--	--	-----------	--------	---------------------	--------------

Anexo VIII – Experiencia en Risk IT

Experiencia en Risk IT

De una experiencia personal del autor en el mundo de las tecnologías de la información, en la pequeña y mediana empresa (PYME), se pone de manifiesto el riesgo inherente a la aplicación de estas tecnologías en el quehacer diario de la empresa.

Siempre que el departamento de las TI, dentro de la pequeña y mediana empresa, se encuentra con obstáculos, debidos a las limitaciones propias del paso del tiempo, a la antigüedad de los equipos, a los cambios de personal, creación de nuevos productos, estrategias o crecimiento de la empresa, se pone de manifiesto el hacer una parada en el tiempo y plantear un nuevo proyecto a futuro que garantice las limitaciones presentes y futuras para la eliminación de los riesgos. Se plantea hacer una Gestión Integral del Riesgo (ERM) y poner en marcha una serie de herramientas para su implantación.

En el [Anexo XV] se presenta el trabajo realizado y los resultados obtenidos del mismo.

Marco de Trabajo

Lo primero que se presentó en el Gobierno de TI fue la limitación de los recursos tecnológicos con los que se contaba en ese preciso momento y que limitaba mucho cualquier mínimo crecimiento o la simple implantación de nuevas aplicaciones de mejora. Se hacía necesario el crecer en recursos, mayor capacidad de proceso, mayor espacio de almacenamiento, mejores comunicaciones, incrementar el número de puestos de trabajo, mayor formación del personal, aplicar las nuevas tecnologías, mejoras del software implementado, seguridad, etc. Era todo un mundo de posibilidades que permitiría gestionar de manera diferente. Si el cambio no se hacía, el futuro empresarial estaba abocado al fracaso. Se necesitaba de una urgentísima actuación, la creación de un marco basado en un conjunto de principios y guías, procesos de negocio y directrices de gestión que se ajustaran a estos principios.

En aquellos tiempos no se disponía de la experiencia compartida, no había libros que hablaran del tema, todo era un nuevo mundo donde si se daba el paso, podíamos encontrarnos con posibilidad de éxito o posibilidad de fracaso. Se trataba de establecer las mejores prácticas para la gestión de riesgos proporcionando un conjunto de controles para mitigar los riesgos de TI.

Se decidió organizar una reunión al más alto nivel con la gerencia, dirección de la empresa, directores de área y jefes. En esa reunión se planteó la situación anterior, su evolución a la situación actual y la situación a futuro. Hubo quien entendió lo expuesto y apostó por la mejora y comprometiéndose al esfuerzo del cambio, pero también surgieron detractores a las soluciones planteadas y asustados por el cambio, ¿tampoco estamos tan mal?, comentaron. Se aprobó por mayoría la determinación de realizar el cambio y arriesgar por el futuro y las mejoras que trajera.

Se hizo un estudio a fondo y en conciencia de toda la compañía. Se estudiaron todos los departamentos, el personal que los componían, los responsables, sus tareas, las interacciones con otros departamentos, relación con clientes y proveedores, relaciones con la dirección.

Estos eventos, planteaban un riesgo y una oportunidad para evaluar el mismo y generar las soluciones oportunas, la dimensión del riesgo, y cómo gestionarlo.

Para la propiedad era un riesgo del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización y que potencialmente podrían afectar el negocio. Supone dificultades para alcanzar las metas y objetivos estratégicos.

Se inicia un proceso de recopilación de todo tipo de información referente a documentos, impresos, flujos de los documentos, tratamiento de la información, su archivo y recursos mecánicos, todo papel que se estuviera utilizando en cada sector de la empresa.

Referente a las TI se valoraron todos los equipos de información y se hizo un inventario de todos los sistemas de que dispone cada departamento.

Se toma información de cada uno de los empleados que pertenecían en ese momento a los diferentes departamentos. Se confirmó el tipo de trabajo que hacían, como lo hacían, con quien lo compartían y se preguntó ¿qué cree usted que está bien y que es lo que hay que mejorar? Se obtuvo un informe completo de lo positivo y negativo de cada puesto de trabajo y de lo que, según el empleado, habría que cambiar, como lo haría si él tuviera autoridad para hacerlo.

Beneficios

Se preparó un marco inicial que fue presentado a la alta dirección.

Este Marco Risk IT [11] pormenorizado se llevó a una reunión de la alta dirección.

Fueron presentados los actuales medios de que se disponía, la vida útil que quedaba con el crecimiento que se estaba soportando, los fallos en algunas áreas de la empresa, tareas repetitivas que se estaban produciendo en ese momento del estudio y necesidades que se daban en ciertas áreas.

También se presentó un plan de mejora continua que incidiría sobre áreas de la empresa que actualmente estaban siendo desatendidas.

Principio de los Riesgos IT

El riesgo del negocio va asociado al uso, influencia, participación y adopción de las TI.

Se estudian los riesgos inherentes al cambio tecnológico y se valoran los pros y los contras de cada área que se va a ver afectada. Riesgo asociado a la capacidad de soportar nuevas tecnologías, programas, formación y sobre todo al cambio.

Se valoran a nivel de Sistemas de TI, que soluciones son las más apropiadas para afrontar el nuevo cambio. Se buscan las de vanguardia, las de última tecnología y las que presenten un futuro mejor donde los posibles costos de nuevos cambios lo soporten sin grandes repercusiones económicas.

Gobierno del Riesgo

Se establece y se mantiene una vista del riesgo común. Se valora la implantación de nuevos sistemas. Que implicación van a tener sobre la empresa, en los departamentos y en las personas y se ve el beneficio final.

Se trata de gestionar el riesgo empresarial. Unos de los apartados más importantes es el costo: la inversión económica, la inversión en tiempo y la inversión en recursos. Se exige un mayor esfuerzo a todas las partes.

Se decide la toma de decisiones, siendo conscientes de los riesgos de negocio. Se tiene que seguir trabajando con la metodología antigua y sistemas antiguos a la vez que se van implantando las nuevas metodologías, los nuevos sistemas, se va formando al personal de la empresa y se van ganando adeptos uno a uno que estén a favor del cambio. También encontramos rechazo, obstáculos, oposiciones fuertes que se niegan a realizar una mejora. Las mejoras no son entendidas

como algo nuevo y que simplificará el trabajo y lo hará menos vulnerable a fallos, sino que para algunos suponen esfuerzo no gratificado, molestias, desgana, aprender, esforzarse. Esto es una lucha quijotesca contra el viento.

Evaluación del riesgo

Se establece una segunda recogida de datos para confirmar que el nuevo plan de gestión cumple todos los requisitos.

Se evalúa nuevamente los riesgos del proyecto. Se repasan y se ajustan a plan maestro.

Se mantiene el perfil definido de riesgo en función de todos los parámetros analizados.

Se mantienen reuniones con los máximos responsables de departamento y se les va informando de todos los pasos que se están dando y próximos a dar.

Respuesta del riesgo

Se articulan una serie de normas a cumplir en cada una de las fases diseñadas y se controlan.

Se estudia la mejor forma de manejar los riesgos que presenta el plan.

Ante los acontecimientos que van surgiendo se reacciona de manera inminente de forma que el impacto del riesgo sea el menor posible.

Se lucha controlando la inversión financiera, los tiempos del cambio, la participación del personal y los propios recursos humanos.

Mejores Prácticas

La aplicación de mejores prácticas proporcionará beneficios tangibles en el negocio como son nuevas iniciativas apoyadas por mayor número de usuarios implicados, menor número de fracasos, aumento de la calidad de la información, aplicaciones innovadoras, más confianza y menos preocupaciones.

Se mejora en seguridad, futuro, calidad, menores consumos de energía, menores costes de ampliación de equipos, menor tiempo en operaciones y programación.

La nueva iniciativa empresarial se verá fortalecida por el riesgo financiero, de menor impacto. El costo de mantenimiento de la antigua estructura se compra con las nuevas soluciones y se comprueba que habrá un menor costo sobre los nuevos sistemas, más seguros y más fiables.

Resultados

Después de una visión precisa del presente y futuro próximo de los riesgos relacionados con las TI en toda la organización y el éxito con el que la organización se ocupa de dichos riesgos.

El proceso de implantación fue realizado de una manera minuciosa implicando a todos los departamentos de la empresa en el proyecto. Se sabía que el éxito del proyecto vendría dado por el grado de implicación de los distintos operadores.

El primer paso consistió en la instalación del nuevo sistema, totalmente distinto al anterior. Fue una migración de un sistema a otro totalmente diferente. Hubo que preparar al personal de TI en el uso y manejo del nuevo sistema. Hubo que aprender el nuevo sistema operativo. Esto supuso un gran

esfuerzo humano y se contó con la predisposición y el sobre-esfuerzo humano que tuvieron que realizar las personas de TI.

Se instalaron nuevas aplicaciones y hubo que familiarizarse con ellas. Las aplicaciones habituales de oficina y comunicaciones. Se formaron los tecnólogos y estos serían los que en una segunda fase formarían a los usuarios finales. Esta segunda fase fue más larga de lo previsto en un principio. El esfuerzo de la migración fue un esfuerzo que no estuvo bien dimensionado en su fase de proyecto. La realidad es que desbordó a todo el personal de TI e hizo que tuvieran un pequeño retraso en el seguimiento del proyecto.

Al mismo tiempo se puso en marcha la implantación de soluciones de software. Se optó por una doble alternativa. Por un lado se contrató externamente la aplicación de Contabilidad y se decidió desarrollar internamente la aplicación de Gestión y Producción. En ese momento la empresa tenía una aplicación de Gestión muy bien ajustada a la realidad y a los planes de futuro. Por tanto la decisión de reprogramar lo existente supondría doble ventaja, el usuario la conocía y podría seguir utilizando la misma dinámica de trabajo y por otro lado el tiempo de programación sería menor. También se contaba con que el tener un desarrollo propio era más ventajoso que el de disponer de uno externo.

La implantación y puesta en marcha de la Aplicación de Contabilidad fue la primera aplicación que se decidió poner en marcha, por el hecho de ser un departamento crítico en la empresa. Se formó al personal del departamento y se estudiaron mejoras aportadas por los usuarios finales. Estos pequeños cambios fueron un mayor riesgo. Por un lado supuso un mayor costo financiero y por otro un mayor costo en recursos humanos. Esto también hizo que se produjeran retrasos sobre plan marcado.

La Aplicación de Gestión fue a la vez iniciada en su desarrollo de programación por el Departamento de IT. El primer paso fue poner en marcha el módulo de Comercial. Su puesta en marcha supondría el principio del eslabón que nos llevaría al éxito.

Los archivos más importantes fueron exportados desde el antiguo sistema al nuevo sistema. Esto supuso un respiro para el departamento implicado ya que la mayoría de su información fue recuperada y presentada de manera fehaciente en nuevo sistema. Como mejoras incorporadas fueron la facilidad de acceso a la información, la mayor velocidad de respuesta a sus peticiones y la obtención de todo tipo de informes y estadísticas que antes no poseían.

El éxito de la puesta en marcha en el Departamento Comercial fue una superación del riesgo y el primer aliciente para entender el esfuerzo que la empresa y todos los implicados estaban haciendo. Era prodigioso ver como un pequeño grupo de personas ilusionadas e implicadas habían conseguido un objetivo común que les pertenecía a todos. Se mejoraron los flujos de información y el rendimiento.

Le siguieron los Departamentos de Compras y de Almacén y Gestión de productos. El siguiente paso fue programar para los Departamentos de Planificación y Producción. El siguiente departamento en poner en marcha fue el de Expediciones. El último departamento fue el de Facturación.

Anexo IX – Ikujiro Nonaka e Hirotaka Takeuchi

Ikujiro Nonaka

Ikujiro Nonaka junto a Hirotaka Takeuchi son autores referentes en el área de la gestión del conocimiento, con reconocidas y prestigiosas publicaciones tanto en forma individual como conjunta. Desarrollaron un trabajo sobre las características particulares del nuevo proceso de desarrollo de producto de las compañías japonesas, cuando participaron en el Coloquio del 75° Aniversario de la Escuela de Negocios de Harvard. En 1986 publicaron el artículo “El nuevo juego del desarrollo de nuevos productos” en la Harvard Business Review. Realizó un doctorado en mercadotecnia y teoría organizacional. En Berkeley estudió sociología, heredando la tradición filosófica de la Universidad que se ve reflejada en las múltiples referencias a la filosofía y epistemología griegas en sus libros. También la tradición intelectual del programa de doctorado de Berkeley, que se inclina hacia el desarrollo de la teoría, ejerció una influencia que se ve reflejada en el intento de formalizar un modelo genérico de creación del conocimiento organizacional. Al dejar Berkeley Ikujiro Nonaka regresa a Japón para impartir clases en la Universidad de Nanzan y más tarde en la Academia de la Defensa Nacional. En 1982, trabajó en la Universidad de Hitotsubashi, donde se vuelve a encontrar con Hirotaka Takeuchi.

En Japón elabora junto a Takeuchi una nueva teoría sobre la creación de conocimiento organizacional, para investigadores y ejecutivos de Occidente.

Hirotaka Takeuchi

Hirotaka Takeuchi trabajó junto a Ikujiro Nonaka. Referentes en el área de la gestión del conocimiento, con reconocidas y prestigiosas publicaciones tanto en forma individual como conjunta. En 1970 inició la Maestría en Administración de empresas (MBA), en Berkeley, donde junto a Nonaka estudiaron sociología, heredando la tradición filosófica de la Universidad que se ve reflejada en las múltiples referencias a la filosofía y epistemología en sus libros, donde intentan formalizar un modelo genérico de creación del conocimiento organizacional. Desarrollaron un trabajo sobre las características particulares del nuevo proceso de desarrollo de producto de las compañías japonesas, cuando participaron en el Coloquio del 75° Aniversario de la Escuela de Negocios de Harvard. Se encuentra nuevamente con Nonaka en 1983 al comenzar a trabajar en la Universidad de Hitotsubashi.

En 1986 publicaron el artículo “El nuevo juego del desarrollo de nuevos productos” en la Harvard Business Review. Posteriormente dictó clases en la Escuela de Administración de Harvard, en donde se centró en estudios de caso.

Trabajo de Nonaka y Takeuchi

Ambos autores plantean en su libro *“La organización creadora de conocimiento: Cómo las compañías Japonesas crean la dinámica de la innovación”* una nueva explicación de por qué algunas firmas japonesas han sido constantemente exitosas en cuanto a innovación se refiere.

Desarrollan un modelo universal de la forma en que una compañía debería ser dirigida, basándose en la convergencia de prácticas de administración japonesas y occidentales.

Argumentan que las compañías japonesas han sido exitosas gracias a sus habilidades y perfeccionamiento en el campo de la “creación de conocimiento organizacional”. Este concepto debe entenderse como la capacidad de una compañía para generar nuevos conocimientos, diseminarlos entre los miembros de la organización y materializarlos en producto, servicios y sistemas. Estas organizaciones se caracterizan por innovar continuamente, en cantidades cada vez

mayores y en espiral. Como ejemplo se plantea el caso de la industria automovilística en donde a través de las innovaciones en tecnologías de procesos fueron los primeros en manejar el concepto de producción “justo a tiempo”, e introdujeron nuevos parámetros de calidad y productividad, logrando tiempos más cortos y una mayor cantidad de clientes satisfechos que las que tenían sus rivales extranjeros.

Plantean las distintas concepciones del conocimiento por parte de las empresas niponas y occidentales. Mientras que las primeras consideran que el conocimiento es principalmente tácito, las segundas lo consideran explícito, formal y sistemático en donde la única manera de pensar en las organizaciones es considerarlas como máquinas de procesamiento de información.

Presentan las ideas fundamentales de lo que es el conocimiento y como se genera, esto permite entender la diferencia básica entre las formas en las que los ejecutivos occidentales y japoneses tratan con la creación del conocimiento. Plantean una descripción de las ideas contrarias sobre epistemología existentes en las tradiciones actuales de Occidente y de Japón. La teoría que presentan se basa en la idea que las dos perspectivas son complementarias. Estos plantean que cualquier teoría de creación de conocimiento que pueda considerarse válida, debe contener elementos de ambas.

Se muestra la diferencia del concepto de individuo y de grupo por parte de los japoneses y los occidentales. Se plantea que si bien es importante entender como las organizaciones crean nuevos productos, nuevos métodos y nuevas formas organizacionales, resulta más necesario entender como generan el nuevo conocimiento que hace posible aquellas creaciones.

Según esta teoría la clave de la creación de conocimiento es la movilización y conversión del conocimiento tácito. Cuando la interacción entre conocimiento tácito y explícito se eleva dinámicamente de un nivel ontológico bajo a niveles más altos, surge una espiral. Plantean cuatro formas de conversión de conocimiento que surgen cuando el conocimiento tácito y el explícito interactúan. Estas cuatro formas a las que llaman socialización, exteriorización, combinación e interiorización, constituyen el motor del proceso de creación de conocimiento.

Se establecen dos dimensiones de creación del conocimiento, la ontológica y la epistemológica.

Se define a la creación de conocimiento organizacional como un proceso en espiral que inicia en el nivel individual y se mueve hacia adelante pasando por comunidades de interacción cada vez mayores, y que cruza los límites o fronteras de las secciones de los departamentos, de las divisiones y de la organización. Plantean que la organización debe posibilitar las condiciones para la creación de conocimiento organizacional a través de la existencia de una intención a la creación de conocimiento, una actuación autónoma por parte de los individuos participantes, una variedad de requisitos, una fluctuación y caos creativo que estimulen la interacción de la organización y el ambiente externo y la existencia de redundancia, esto significa la existencia de información que va más allá de los requerimientos operacionales inmediatos de los miembros de la organización.

Los autores presentan un modelo de cinco fases del proceso de creación de conocimiento organizacional. La primera fase es la de compartir conocimiento tácito la cual corresponde rudimentariamente a la socialización, la segunda es la de crear conceptos, proceso que es similar a la exteriorización, la tercera fase consiste en justificar los conceptos creados en la fase anterior para determinar si en verdad vale la pena desarrollar el nuevo concepto.

Después de ser aceptados los conceptos, en la cuarta fase los conceptos son convertidos en un arquetipo, que puede adoptar la forma de un prototipo si se trata del desarrollo de un producto físico, o de un mecanismo operacional si se trata de una innovación abstracta, como un valor corporativo, un nuevo sistema administrativo o una estructura organizacional innovadora. La última fase consiste en distribuir el conocimiento de forma cruzada, esto consiste en distribuir el

conocimiento creado, por ejemplo en una división, entre otras personas de la misma división, a través de otras divisiones o hasta en grupos de interés externos.

Presentan en sus trabajos el caso de la compañía Japonesa, Matsushita Electric Industrial Co., Ltd sobre el desarrollo de un aparato para hacer pan, conocido como Home Bakery (panificadora casera) y el efecto que tuvo en la compañía, donde se generó un proceso continuo de creación de conocimiento a nivel corporativo, donde el conocimiento tácito es movilizado en la búsqueda de la innovación creativa como fuente de ventajas competitivas sostenibles.

Se presentan las cuatro formas de conversión de conocimiento, las condiciones que lo hacen posible, así como las cinco fases de creación de conocimiento. También el caso muestra como el conocimiento creado a través del desarrollo de la panificadora casera fue elaborado en el interior de Matsushita, resultando en una espiral de creación de conocimiento más amplia.

Los autores plantean un nuevo modelo denominado “centro-arriba-abajo” para la administración del conocimiento utilizado en las compañías Japonesas. Este modelo ubica al ejecutivo de nivel medio en el centro de la administración de conocimiento, justo en la intersección de los flujos de información horizontal y vertical de la compañía, a diferencia de los modelos tradicionales (arriba-abajo y abajo-arriba) y redefine los papeles de los altos directivos y de los empleados de primera línea.

Algunos casos de estudio muy interesantes que ilustran los modelos tradicionales son General Motors (arriba-abajo) y 3M (abajo-arriba), y el de las empresas niponas como el caso de Honda con el proyecto del City y el de Canon a través del desarrollo de su producto mini-copiadora para describir los papeles que deben desempeñar los participantes clave en el modelo centro-arriba-abajo.

Los autores presentan una estructura organizacional que sustenta el proceso de administración para la creación de conocimiento llamada hipertexto, que permite a la organización crear conocimiento de forma eficaz y efectiva. Plantean que los dos tipos de organización tradicionales, burocracia y fuerza estratégica, no son adecuadas para la creación de conocimiento, requiriéndose una combinación o síntesis de las mismas a través del hipertexto. La organización de tipo hipertexto está formada por capas o contextos interconectados: el sistema de negocios, el equipo de proyectos y la base de conocimientos. La característica central de la organización de tipo hipertexto es la habilidad que tienen sus miembros para cambiar el contexto. Se ve representada esta estructura a través del caso de la organización Kao como un modelo de transición y el de la organización Sharp como un modelo más perfeccionado.

Los autores analizan cómo se da la creación de conocimiento organizacional en una escala global, planteando las diferencias entre las formas de considerar la creación de conocimiento organizacional en Japón y en Occidente y la importancia decisiva que tiene la socialización y la exteriorización para la creación de conocimiento global. Existen dos casos prácticos de creación de conocimiento organizacional global, como ser el modelo de automóvil “Primera” en la organización Japonesa Nissan y el de las palas hidráulicas “REGA” de Shin Caterpillar Mitsubishi, alianza estratégica de dos organizaciones una Japonesa y la otra americana.

Otros trabajos de Nonaka

Nonaka junto a R. Toyama y N. Konno presentaron un artículo sobre un modelo unificado de creación dinámica del conocimiento (“A Unified Model of Dynamic Knowledge Creation”), ya que plantean que no se entiende claramente el concepto de conocimiento y su proceso de creación.

Indican que la “Gestión del conocimiento” de la que los académicos y empresarios hablan a menudo significa solamente “Gestión de la información”. Tradicionalmente se ha considerado a la organización como una máquina de procesamiento de información que toma y procesa la información del entorno para solucionar un problema y se adapta al entorno en función de una meta establecida. Esta visión estática y pasiva de la organización no permite capturar el verdadero proceso dinámico de la creación del conocimiento en el cual las organizaciones no solucionan únicamente problemas sino que crean y definen problemas, desarrollan y aplican nuevo conocimiento para solucionar los problemas, y entonces desarrollan nuevo conocimiento a través de la acción de solucionar los problemas. La organización no es meramente una máquina de procesar información, sino una entidad que crea el conocimiento mediante la acción y la interacción. Interactúa con su entorno, redefine el entorno y aún a sí misma mediante el proceso de la creación del conocimiento.

Por lo tanto el aspecto más importante para entender la capacidad de una firma concerniente al conocimiento, es la capacidad dinámica de crear continuamente nuevo conocimiento a partir de las capacidades específicas ya existentes en la firma, en lugar del almacenaje de conocimiento (tal como una tecnología en particular) que una firma posee en un momento específico. Solo a través de esta visión de organización como entidad que crea conocimiento continuamente es que estas podrán entender, crear y gestionar el conocimiento.

Presentan la organización como una entidad que crea conocimiento a través de la acción y la interacción. Interactúa con su entorno y adapta el entorno y hasta sí misma a través del proceso de creación de conocimiento. La creación del conocimiento en la organización se realiza en forma de espiral entre conceptos aparentemente antitéticos como por ejemplo, tácito y explícito o micro y macro. Los autores argumentan que la clave para dirigir el proceso de creación del conocimiento es el pensamiento dialéctico, que trasciende y sintetiza tales contradicciones. El conocimiento en las organizaciones es creado a través de interacciones sociales entre individuos y organizaciones, es por ello que es dinámico. Es específico al contexto, y depende de un tiempo y espacio particular.

El conocimiento es dinámico, ya que es creado a través de las interacciones sociales de individuos y organizaciones. El conocimiento es específico a un contexto, y depende de un tiempo y espacio particular. Es humanístico, al estar esencialmente relacionado a la acción humana. Tiene las naturalezas activas y subjetivas representadas por los términos como compromiso y creencia que están profundamente arraigadas al sistema de valores del individuo.

La información se vuelve conocimiento cuando es interpretada por individuos, se le da un contexto, y se ancla en las creencias y compromisos de los individuos. Por tanto, el conocimiento es relacional: cosas tales como "verdad", "bondad" y "belleza" están en el ojo del observador. Plantean la existencia de dos tipos característicos de conocimiento: explícito y tácito. El conocimiento explícito puede ser expresado en lenguaje formal, sistemático y compartido en forma de datos, fórmulas científicas, especificaciones, manuales y similares. Puede ser procesado, transmitido y almacenado de forma relativamente fácil. En contraste, el conocimiento tácito es altamente personal y difícil de formalizar y comunicar. Las visiones subjetivas, intuiciones y corazonadas caen en esta categoría de conocimiento. El conocimiento tácito está profundamente arraigado en las acciones, procedimientos, rutinas, compromisos, ideales, valores y emociones. Está incorporado en una profunda percepción del cuerpo y la mente humana. Sin la visión tácita el conocimiento explícito pierde rápidamente su significado.

La expresión escrita solamente es posible luego de que se ha desarrollado la expresión interna. La interacción de ambos tipos de conocimiento permite la creación del conocimiento.

Para entender cómo las organizaciones crean el conocimiento dinámicamente, los autores proponen un modelo de creación de conocimiento que consiste en tres elementos:

El proceso SECI: Es el proceso de creación de conocimiento a través de la conversión entre conocimiento tácito y explícito.

Ba: el contexto compartido para la creación de conocimiento. La plataforma donde se da la conversión del conocimiento.

Bienes de conocimiento: Las entradas, las salidas y moderadores del proceso de creación de conocimiento (controlan el crecimiento del conocimiento a través del proceso de conversión continua del conocimiento y moderan el desempeño de Ba como plataforma de SECI).

Los tres elementos de la creación del conocimiento tienen que interactuar entre sí para formar el espiral del conocimiento que crea el conocimiento.

El proceso SECI (Socialización, Externalización, Combinación, Internalización) plantea que una organización crea el conocimiento mediante la interacción entre el conocimiento explícito y el tácito. Se llama a la interacción entre los tipos de conocimiento "la conversión de conocimiento". A través del proceso de conversión el conocimiento tácito y el explícito se expanden tanto en calidad como en cantidad. Hay cuatro modos de conversión del conocimiento y son: a- socialización (de conocimiento tácito a conocimiento tácito), b- externalización (de conocimiento tácito a conocimiento explícito), c- combinación (de conocimiento explícito a conocimiento explícito), y d- internalización (de conocimiento explícito a conocimiento tácito).

Modos de conversión del conocimiento:

Socialización: Es el proceso de conversión de nuevo conocimiento tácito a través de experiencias compartidas. Un ejemplo de socialización ocurre típicamente en el aprendizaje tradicional, donde los aprendices aprenden el conocimiento tácito requerido en su oficio mediante las experiencias manuales, en lugar de los manuales o los libros de texto escritos.

Externalización: Es el proceso de articular el conocimiento tácito en conocimiento explícito. Cuando el conocimiento tácito se vuelve explícito, el conocimiento se cristaliza, permitiendo así que sea compartido con otros, y así se convierte en la base de nuevo conocimiento. Un ejemplo es el círculo de control de calidad, que les permite a los empleados mejorar los procesos de manufactura mediante la articulación de conocimiento tácito acumulado luego de años de trabajo favoreciendo la mejora continua. La conversión exitosa de conocimiento tácito en conocimiento específico depende del uso secuencial de la metáfora, la analogía y el modelo.

Combinación: Es el proceso de convertir el conocimiento explícito en series más complejas y sistemáticas de conocimiento explícito. El conocimiento explícito es obtenido desde dentro y fuera de la organización y entonces combinado, editado o procesado para formar nuevo conocimiento. El nuevo conocimiento explícito es entonces diseminado entre los miembros de la organización. El uso creativo de las redes de comunicaciones computarizadas y las bases de datos de gran escala pueden facilitar este modelo de conversión de conocimiento. Un ejemplo es cuando el administrador de la compañía almacena información de toda la organización y la pone junta en un contexto para crear un reporte financiero, este reporte es nuevo conocimiento en el sentido de que sintetiza el conocimiento de muchas fuentes diferentes en un contexto.

Internalización: La internalización es el proceso de incorporar el conocimiento explícito al conocimiento tácito. Mediante la internalización, el conocimiento explícito creado es compartido a través de la organización y convertido en conocimiento tácito por los individuos. La internalización está muy relacionada con "aprender al hacer". Por ejemplo, los programas de entrenamiento pueden ayudar a los entrenados a entender una organización y a sí mismos. Al leer los documentos y los manuales sobre sus trabajos y la organización, y al reflexionar sobre ellos, los entrenados internalizan el conocimiento explícito descrito en tales documentos para enriquecer su base de

conocimiento tácito. El conocimiento explícito también puede ser incorporado mediante simulaciones o experimentos que disparen el aprender al hacer.

Ba es el contexto compartido en el cual el conocimiento es compartido, creado y utilizado. En la creación de conocimiento, la generación y regeneración del Ba es la clave, ya que provee la energía, calidad y lugar para llevar a cabo las conversaciones individuales y para llevar adelante el espiral de conocimiento. Ba es un lugar donde la información es interpretada para convertirse en conocimiento. Significa un tiempo y espacio específico (físico, virtual, mental) en el que los participantes comparten la creación de nuevo conocimiento. Ba es dinámico, cambiante, trasciende el tiempo y el espacio y provee a los participantes de otros puntos de vista. La construcción, el mantenimiento y la utilización de Ba es importante para facilitar el crecimiento del conocimiento organizacional.

Existen cuatro tipos de Ba con diversas características que interactúan para favorecer la creación de conocimiento (Ba Originador, Ba Dialogador, Ba Sistematizador y Ba Ejercitador). Son definidos por dos dimensiones de interacciones. Una dimensión es el tipo de interacción, esto es, si la interacción tiene lugar individual o colectivamente. La otra dimensión es el medio utilizado en tales interacciones, esto es, si la interacción es mediante contacto cara a cara o mediante medios virtuales tales como libros, manuales, memos, e-mails o teleconferencias. Cada Ba ofrece un contexto para un paso específico en el proceso de la creación de conocimiento mediante las respectivas relaciones, aunque cada Ba es individual y los modos de conversión no son de ninguna forma exclusivos. El edificar, mantener y utilizar Ba es importante para facilitar la creación del conocimiento organizacional. Por lo tanto es muy importante entender las diferentes características de Ba y cómo interactúan entre sí.

El concepto de Ba parece tener algunas singularidades con el concepto de comunidades de práctica. Basado en el modelo de aprendizaje, el concepto de comunidades de práctica sostiene que los miembros de la comunidad aprenden mediante su participación en las comunidades y la memorización gradual de las tareas. De cualquier forma hay diferencias importantes entre los conceptos de las comunidades de práctica y Ba.

Mientras que una comunidad de práctica es un lugar donde los miembros aprenden el conocimiento que está inmerso en la comunidad, Ba es un lugar donde se crea nuevo conocimiento. Mientras que el conocimiento ocurre en cualquier comunidad de práctica, Ba necesita energía para llegar a ser un Ba activo donde se crea conocimiento. El límite de una comunidad de práctica está firmemente establecido por la tarea, la cultura y la historia de la comunidad. La continuidad y la consistencia son importantes para la comunidad de práctica, ya que necesita una identidad. En contraste, el límite de Ba es fluido y puede ser cambiado rápidamente al ser establecido por los participantes. En lugar de estar limitado por la historia, Ba tiene una calidad de "aquí y ahora". Esta constantemente en movimiento. Es creado, funciona y desaparece de acuerdo a la necesidad. Ba cambia constantemente, ya que los contextos de los participantes o la membrecía del Ba cambian. En una comunidad de práctica, los cambios principalmente tienen lugar a un nivel micro (individuo), mientras los nuevos participantes aprenden a ser participantes completos. En Ba, los cambios tienen lugar tanto en el nivel micro como el macro, ya que los participantes cambian tanto a nivel individual como al propio Ba.

Mientras que la membrecía de la comunidad de práctica es bastante estable, y toma tiempo para que un nuevo participante aprenda sobre la comunidad para convertirse en un participante completo, la membrecía de Ba no está fijada; los participantes vienen y van. Mientras que los miembros de la comunidad de práctica pertenecen a la comunidad, los participantes de Ba se relacionan con el Ba.

Aunque el conocimiento se considera uno de los bienes más importantes para una firma, para crear una ventaja competitiva sostenible hoy en día, aún no poseemos un sistema y herramientas efectivas para evaluar y gestionar los bienes de conocimiento. Aunque una variedad de medidas han sido propuestas, los sistemas de contabilidad existentes son inadecuados para capturar el valor de los bienes de conocimiento, debido a la naturaleza tácita del conocimiento. Los bienes de conocimiento deben ser edificados y utilizados internamente para que su valor completo pueda ser comprendido, ya que no pueden ser prontamente comprados ni vendidos. Necesitamos edificar un sistema para evaluar y gestionar los bienes del conocimiento en una firma de forma más efectiva. Otra dificultad al medir los bienes de conocimiento es que son dinámicos. Los bienes de conocimiento son tanto entradas como salidas y factores moderadores de las actividades creadoras de conocimiento de una organización, por lo cual están constantemente evolucionando. El tomar una instantánea de los bienes de conocimiento que la organización posee en un momento puntual nunca es suficiente para evaluar y gestionar los bienes de conocimiento apropiadamente.

Los autores categorizan los bienes de conocimientos en cuatro tipos: Bienes de conocimiento experimental, conceptual, sistémico y rutinario, los cuales forman la base del proceso de creación de conocimiento. Los bienes de crecimiento experimental consisten en el conocimiento tácito compartido que es creado mediante experiencias manuales compartidas entre los miembros de la organización y sus clientes, proveedores y firmas afiliadas. Ejemplo de este bien de conocimiento es el “saber que hacer”, conocimientos adquiridos y acumulados por los individuos durante las experiencias de trabajo. Estos bienes permiten el logro de una ventaja competitiva sostenible para la organización dada su naturaleza tácita. Los bienes de conocimiento conceptual consisten en conocimiento explícito articulado mediante imágenes, símbolos y lenguaje. Son los bienes basados en los conceptos pertenecientes a los clientes y miembros de la organización. Ejemplos de estos bienes son la equidad de marca, que es percibida por los clientes y los conceptos o diseños que son percibidos por la organización. Estos bienes de conocimiento son más fáciles de sostener que los bienes de conocimiento experimental debido a que tienen formas tangibles, aunque aún sea difícil comprender lo que los clientes y los miembros de la organización perciben. Los bienes de conocimiento sistémico consisten en conocimiento explícito sistematizado y empacado, tal como tecnologías explícitamente declaradas, especificaciones de producto, manuales, e información documentada y empacada sobre clientes y proveedores.

Las propiedades intelectuales legalmente protegidas tales como licencias y patentes también caen dentro de esta categoría. Pueden ser transferidos de forma relativamente fácil ya que es el tipo de bien de conocimiento más visible. Los bienes de conocimiento rutinario consisten en el conocimiento tácito que es convertido en rutina y está incorporado en las acciones y prácticas de la organización. A través de continuos ejercicios, ciertos patrones de pensamiento y acción son reforzados y compartidos entre los miembros de la organización.

El “saber cómo”, la cultura organizacional y las rutinas organizacionales para llevar adelante los deberes del día a día son ejemplos de los bienes de conocimiento rutinario. Una característica de los bienes de conocimiento rutinario es que son prácticos.

El proceso de creación de conocimiento no puede ser gestionado en el sentido tradicional de “gestión”, que se centra en controlar el flujo de la información. Los administradores pueden, de cualquier forma, llevar a la organización a crear conocimiento activa y dinámicamente proveyendo ciertas condiciones. Los roles de los administradores altos y medios son muy importantes para llevar adelante un proceso dinámico de creación de conocimiento.

Es especialmente importante para el proceso de creación de conocimiento el rol de los productores de conocimiento, esto es los administradores medios que están en la intersección de los flujos verticales y horizontales de información de la compañía e interactúan activamente con otros para crear conocimiento mediante su participación o liderazgo en Ba. En la creación de conocimiento, el “liderazgo distribuido” que se ve en “la gestión centro-arriba-abajo” es la clave ya que no puede ser

gestionado mediante el liderazgo tradicional de arriba hacia abajo. La gestión media y alta toma el rol de liderazgo mediante una “lectura” de la situación, así como liderando el trabajo en los tres elementos del proceso de creación de conocimiento. Los líderes proveen la visión del conocimiento, desarrollan y promueven la distribución de los bienes de conocimiento, crean y energizan el Ba, y habilitan y promueven el espiral continuo de creación de conocimiento. Es especialmente importante la visión de conocimiento, que afecta las tres capas del proceso de creación del conocimiento. Para crear conocimientos dinámica y continuamente, una organización necesita una visión que sincronice a la organización entera. Es el rol de la alta administración el articular la visión de conocimiento y comunicarla dentro y fuera de la compañía. Debido a que el conocimiento es irrestricto, cualquier forma de conocimiento puede ser creada sin importar la estructura de negocios existente de la compañía. Por tanto es importante que la alta administración articule una visión de conocimiento que trascienda los límites de los productos, las divisiones, las organizaciones y los mercados existentes.

Sirviendo como puente entre las ideas visionarias de aquellos que están arriba y la realidad caótica de la primera línea, el centro tiene entonces que desarmar los valores y visiones creados por los superiores en conceptos e imágenes que guíen el proceso de creación de conocimiento con vitalidad y dirección. Los administradores medios trabajan como productores de conocimiento para recrear la realidad, o para producir nuevo conocimiento de acuerdo con la visión de la compañía. Basado en la visión de conocimiento de la compañía, la administración tiene que facilitar una creación de conocimiento dinámica tomando el rol de guía en la gestión de los tres elementos del proceso de creación de conocimiento. Primero la administración tiene que desarrollar y gestionar los bienes de conocimiento de la compañía, que forman la base del proceso de creación de conocimiento. Recientemente muchas compañías han creado la posición de oficial en jefe de conocimiento (CKO) para llevar adelante esta función. De cualquier forma el rol de estos CKO ha estado hasta ahora limitado a gestionar los bienes de conocimiento como un recurso estático que debe ser explotado. La administración debe jugar un rol más activo facilitando el proceso dinámico de crear bienes de conocimiento a partir del conocimiento.

Anexo X – Estrategia de Gestión del Conocimiento

En la estrategia de codificación el conocimiento es codificado y guardado en bases de datos, donde se puede acceder fácilmente.

La estrategia de personalización está atada a la persona que lo maneja y es transmitido de forma directa.

Para crear valor al cliente, es eficiente el uso del conocimiento codificado cuando se trata de problemas similares, apoyándose en la economía por re-uso. Así como el uso del conocimiento personalizado cuando no se tienen soluciones claras, cuando se enfrenta a problemas únicos, apoyándose en la economía por experiencia.

Según la estrategia definida, la contratación de personal se puede ver modificada, dado que en una estrategia de codificación, el personal se va a entrenar y recibir capacitación dentro de la empresa. En un enfoque de personalización, se contratará personal graduado a nivel de master, con habilidades para compartir conocimiento persona-persona.

Estas estrategias no solo aplican a consultoras, también en centros de salud, empresas de computación, entre otros.

Acces Health es un ejemplo de centro de salud que plantea una estrategia de codificación, donde utiliza un call center en base a un repositorio de conocimiento. Cuando un cliente llama le recomienda un remedio, la visita a determinado médico o pase a la sala de emergencia.

A su vez, con una estrategia de personalización el centro de salud Memorial Sloan-Kettering Cancer Center, cuenta con varios expertos que se consultan por cada caso de cada paciente.

Como ejemplo de empresas de computación podemos ver a Dell cuya estrategia se basa en montar PC's de bajo costo que se fabrican por pedido y se venden directamente al usuario. Plantea el reuso del conocimiento, lo que lo llevó a bajar los costos y cobrar menos que la competencia. Otro caso es el de HP, que utiliza una estrategia de personalización que busca vender productos innovadores.

Las estrategias de gestión también pueden variar el modelo de incentivos a utilizar en la empresa, donde en el caso de la estrategia de codificación se busca recompensar a quienes escriban sus conocimientos y los pongan en el repositorio. Por otra parte para la estrategia de personalización, se recompensan a quienes comparten sus conocimientos de forma directa con otras personas.

El uso de las tecnologías de información, se hace crítico para una estrategia de codificación, ya que se requiere la implementación de un sistema donde codificar el conocimiento. En el caso de la estrategia de personalización se debe implementar un sistema que ayude a las personas a encontrar otras.

Para la elección de la estrategia en una empresa y lograr en base a ésta el beneficio de la empresa y el consumidor, se deberían de responder las preguntas:

¿La empresa ofrece productos estandarizados o personalizados?

¿Se tiene un producto innovador o maduro?

¿Las personas en la empresa utilizan conocimiento explícito o tácito para resolver los problemas?

Anexo XI – Chief Knowledge Officer

El Gerente del Conocimiento (CKO, por su acrónimo en Inglés de Chief Knowledge Officer), es el principal responsable de la gestión del conocimiento en las organizaciones. Es el encargado de iniciar, impulsar y coordinar los programas de Gestión del Conocimiento.

Su perfil coincide con el de líder y emprendedor. Son positivos, entusiastas y tienen la facilidad de transmitir su entusiasmo a los demás.

El CKO tiene la personalidad propia de un líder, es un comunicador natural, manejador de conflictos y catalizador del cambio.

Dado que las características de las funciones que debe llevar a cabo el CKO no implican que este sea un experto en TI ni en Recursos humanos, es fundamental que sus tareas estén alineadas con las que competen tanto al CIO como al CHRO ya que de no ser así la implementación de proyectos de gestión de conocimiento puede verse seriamente limitada. Es necesario que el cambio cultural que implica la gestión de conocimiento se realice en forma alineada con objetivos comunes y utilizando la tecnología para favorecer el logro de los mismos.

Diferencias entre CIO y CKO

Donde exista un CKO, es muy probable que se trate de un CIO. Esto se explica ya que inicialmente los proyectos KM corrientemente fueron asociados al área de TI.

Lo que hace diferente a un CKO de un CIO es el objeto propio de Gestión de cada uno de ellos. Mientras que el CIO tiene como objetivo supervisar el despliegue de las TI, el CKO focaliza su accionar en maximizar la creación, el descubrimiento y la diseminación de conocimientos en la organización.

¿Por qué es necesario un CKO?

Cada vez las empresas tienen una mayor necesidad de contar con un CKO. Esto se debe a que en la actualidad no se puede eludir la necesidad de:

- Maximizar el retorno de las inversiones en conocimiento, tales como nuevas contrataciones, procesos y capital intelectual.
- Explotar los activos intangibles, tales como el know-how, las patentes y la relación de clientes.
- Repetir los éxitos pasados y compartir mejores prácticas.
- Mejorar la innovación (Comercialización de ideas).
- Evitar la pérdida de conocimiento y las fugas producidas por las reestructuraciones organizacionales.

Solamente en los siguientes casos el CKO no es absolutamente prescindible:

- El conocimiento no es importante en el negocio.
- Se está contento con las iniciativas locales (proyectos KM informales) y se espera que todo vaya bien.
- Existe ya una cultura que facilita el compartir conocimiento y un proceso sistémico de difusión.
- El liderazgo en conocimiento viene de la cima y es perseguido apasionadamente.
- Cada uno posee planes de desarrollo de conocimiento en sus planes de trabajo.

- Los sistemas de monitoreo de rendimiento poseen una dimensión explícita en torno al conocimiento.

Para determinar la existencia de un CKO en la organización se deberá analizar las condiciones favorables y desfavorables presentadas anteriormente como complementarias. El considerar sólo algunas establece un criterio parcial que debilita potenciales puntos generadores de una verdadera cultura de aprendizaje organizacional.

Sin embargo, es muy probable que sean las decisiones estratégicas de conocimiento, más precisamente una estrategia de conocimiento las que definan las situaciones a las que se deberá enfrentar el CKO.

El trabajo del CKO en la organización implica muchas expectativas ya que implica el logro de los cambios en la conducta organizacional y gerencial para administrar los conocimientos necesarios para lograr los objetivos del negocio de la organización.

Necesidad de Integración entre CKO, CIO y CHRO

Dado que las características de las funciones que debe llevar a cabo el CKO no implican que este sea un experto en TI ni en Recursos humanos, es fundamental que sus tareas estén alineadas con las que competen tanto al CIO como al CHRO ya que de no ser así la implementación de proyectos de gestión de conocimiento puede verse seriamente limitada. Es necesario que el cambio cultural que implica la gestión de conocimiento se realice en forma alineada con objetivos comunes y utilizando la tecnología para favorecer el logro de los mismos.

Anexo XII – Relación entre Gestión del Conocimiento y Gobierno de TI

Las decisiones sobre los principios de TI que define una organización dependerán del conocimiento que existe y el que debe existir en la organización de manera que TI puede apoyar a la gestión de este conocimiento. Los principios de TI deberán proveer a la organización de la información adecuada en el tiempo necesario para que esta cumpla con sus objetivos. Esta información permitirá el logro del conocimiento necesario para la operativa de la organización así como una buena gestión del mismo para el logro de ventajas competitivas sostenibles.

Los principios de TI deberán estar alineados a la estrategia de la organización para que esta pueda lograr sus objetivos de negocio. Esto solo es posible si se cumple eficientemente el área de enfoque de alineación estratégica del Gobierno de TI, asegurando el enlace de los planes del negocio y de TI. Para poder cumplir eficientemente con la estrategia de negocios definida y establecer adecuadamente los principios de TI, las organizaciones deben alinear los conocimientos, habilidades y capacidades necesarias a través del proceso de alineación estratégica de la gestión del conocimiento.

Uno de los factores que inciden en la elección de la estrategia en una organización es la tecnología. Esto significa lo importante que es para la organización el contar con una tecnología de la información eficiente que posibilite a través de un buen Gobierno de TI una adecuada gestión del conocimiento que permita el cumplimiento de los objetivos estratégicos de la organización.

La adecuada identificación del conocimiento estratégico para la organización, del conocimiento que existe en la organización y de las brechas de conocimiento entre ambos, así como de la incorporación eficiente del conocimiento adquirido desde fuentes externas a la organización o mediante la creación y desarrollo de conocimientos generados internamente, permitirán la correcta definición y la adecuada implementación de los principios de TI.

Según trabajos de investigación realizados sobre el Alineamiento estratégico de TI con los objetivos del negocio en Pymes de Uruguay, se identifica que la toma de decisiones compartida entre el director general (CEO), el director de TI (CIO) y el director financiero (CFO) favorece el alineamiento estratégico de TI con los objetivos del negocio.

Esto se debe a que se requiere un adecuado nivel de conocimiento de TI y del negocio en la organización para que las decisiones de TI estén alineadas con los objetivos del negocio. Para este fin se necesita compartir el conocimiento mediante la diseminación del mismo a través de los expertos en conocimiento de TI y del negocio como lo son el CIO, el CEO y el director general.

Aquí ocurre el proceso de diseminación de gestión del conocimiento.

También es necesaria una culturización organizacional que posibilite el conocimiento a toda la organización sobre los principios de TI definidos, ya que cuando forman parte del lenguaje interno de la organización pueden ser apoyados, analizados, discutidos y pueden evolucionar. Esta culturización es importante para lograr el alineamiento estratégico de TI con los objetivos del negocio. Esto significa la diseminación del conocimiento que debe ser distribuido y compartido a través de los diferentes niveles organizacionales para que todos los integrantes de la organización conozcan sus objetivos y su dirección estratégica, contribuyendo de esta manera al logro de los mismos. Se presenta aquí el proceso de diseminación de gestión del conocimiento.

Para poder tomar buenas decisiones que posibiliten el alineamiento estratégico de TI a los objetivos del negocio (fase de alineación estratégica del Gobierno de TI) y el logro de ventajas competitivas sostenibles para la organización, es necesario contar con el conocimiento adecuado. Esto se logra a través del proceso de identificación de gestión del conocimiento por medio de la identificación del conocimiento que es estratégico para la organización y mediante la construcción de un inventario de los conocimientos, habilidades y experiencia existentes en la organización para determinar sus capacidades actuales y los conocimientos necesarios a incorporar a través del proceso de

incorporación de gestión del conocimiento, para poder lograr la alineación de estos conocimientos con la estrategia de la organización a través del proceso de alineación estratégica de gestión del conocimiento y cumplir con los objetivos del negocio de la organización.

También es importante para tomar buenas decisiones, contar con la mayor cantidad y calidad de información precisa, rápida y efectiva, que le sirva a la organización para definir situaciones actuales y prepararse para las futuras, tomando como ejemplo situaciones de similares características, es decir poder reutilizar el conocimiento.

Para ello no solo es necesario la incorporación del conocimiento sino también el mantenimiento del conocimiento existente en la organización y la continuidad del mismo a través del proceso de preservación de gestión del conocimiento.

A su vez para que el conocimiento pueda ser utilizado, debe ser distribuido y compartido a través de los diferentes niveles organizacionales mediante el proceso de diseminación de gestión del conocimiento.

Las decisiones sobre la arquitectura de TI definidas en el Gobierno de TI, implican decisiones sobre la organización lógica para datos, aplicaciones e infraestructura, con el objetivo de conseguir la integración y estandarización técnica y lograr el negocio deseado. Se determinan las elecciones técnicas en TI para cumplir con los principios de TI definidos previamente. En esta etapa el Gobierno de TI debe lograr una buena gestión del conocimiento ya que la definición del tipo de arquitectura responderá a las necesidades de conocimiento que la organización requiera para su negocio así como a la manera en que se gestiona este conocimiento.

En la toma de decisiones para definir la arquitectura en el Gobierno de TI, se debe tener en cuenta los siguientes procesos de gestión del conocimiento:

identificación del conocimiento, ya que el conocimiento estratégico para la organización requiere de una arquitectura adecuada que le de soporte de manera eficiente; la incorporación del conocimiento, dado que la arquitectura debe permitir la incorporación de conocimiento y experiencia en la organización a través de la adquisición de conocimientos desde fuentes externas a la organización o mediante la creación y desarrollo de conocimientos generados internamente; la preservación del conocimiento, dado que la arquitectura debe contemplar todas las actividades referentes a mantener el conocimiento existente en la organización y asegurar la continuidad del mismo; la diseminación del conocimiento, ya que una buena arquitectura debe posibilitar que se distribuya y comparta conocimiento a través de los diferentes niveles organizacionales para que el uso del conocimiento sea efectivo; la utilización del conocimiento, que consiste en la aplicación y utilización de las mejores prácticas y las lecciones aprendidas capturadas de proyectos anteriores disponibles en el repositorio de lecciones aprendidas y de mejores prácticas, aplicando y utilizando de esta manera los nuevos conocimientos creados o adquiridos.

Las decisiones sobre la infraestructura de TI definidas en el Gobierno de TI, implican decisiones sobre la capacidad de TI con la que cuenta el negocio, tanto a nivel humano como tecnológico.

La infraestructura está presente a lo largo de toda la empresa como servicios fiables y compartidos y utilizados por varias aplicaciones.

En esta etapa el Gobierno de TI debe lograr una buena gestión del conocimiento ya que la definición del tipo de infraestructura responderá a las necesidades de conocimiento que la organización requiera para su negocio así como a la manera en que se gestiona este conocimiento.

La definición de las capacidades de TI con las que cuenta el negocio y las que necesitara tener en el futuro, dependen de las capacidades necesarias para incorporar, preservar, diseminar y utilizar el

conocimiento requerido para lograr los objetivos del negocio. En este sentido se debe alinear la estrategia de negocios con el conocimiento estratégico.

Capacidades de gestión del conocimiento (incorporar, preservar, diseminar y utilizar) inciden en el riesgo de no contar con las capacidades necesarias para el logro de los objetivos del negocio.

En la toma de decisiones sobre la infraestructura de TI a través del Gobierno de TI, se deben establecer los recursos tecnológicos necesarios para lograr el conocimiento requerido y los recursos humanos, principal activo intangible de una organización. Son estas personas a través de sus conocimientos, habilidades y experiencia las que van a posibilitar la incorporación, preservación, diseminación y utilización del conocimiento a través de la tecnología para lograr los objetivos organizacionales. Por tal motivo, es muy importante la adecuada selección e incorporación de los recursos humanos según sea el conocimiento requerido de los mismos y la posibilidad de aprendizaje de estos para el logro del conocimiento estratégico.

Es muy importante la adecuada selección e incorporación de los recursos humanos según sea el conocimiento requerido de los mismos y la posibilidad de aprendizaje de estos para el logro de los objetivos del negocio.

En relación a las decisiones del Gobierno de TI en el área de las necesidades de aplicaciones, estas dependen mucho del conocimiento que se tenga en la organización así como del conocimiento que sea necesario lograr y la forma en que este se gestiona para cumplir con los objetivos del negocio. Las decisiones en ésta área directamente generan valor al negocio, ya que tienen el potencial de beneficiar los objetivos estratégicos del mismo.

Aplicar gestión del conocimiento y la experiencia en ingeniería de software reporta beneficios como realizar más rápido las actividades de ingeniería de software, mejorar la calidad de los procesos, reconocer posibles problemas más rápido, combinar tareas de manera más eficiente y mejorar el desempeño competente de las personas (Schneider, 2009).

De esta manera al ser la ingeniería de software un área que pone en práctica y representa los principios del Gobierno de TI, una adecuada gestión del conocimiento y la experiencia trae beneficios a la Gobernanza de TI.

El objetivo del desarrollo o la compra de las aplicaciones es poder gestionar eficientemente la información a través de las TI de manera de que la organización logre una gestión del conocimiento más eficiente a través de sus procesos de incorporación, preservación, diseminación y utilización.

De esta manera la organización contará con conocimientos no solo operativos sino también de soporte al negocio, que favorecerán la adecuada toma de decisiones, posibilitando el alineamiento de la estrategia del negocio con la estrategia de TI y con el conocimiento estratégico.

En las decisiones de inversiones de TI a través del Gobierno de TI, se debe conocer el estado de la situación actual del negocio para poder determinar el grado de alineamiento estratégico de TI con la estrategia del negocio existente en la organización y así poder tomar decisiones de inversión en TI adecuadas a la estrategia de TI y a los objetivos del negocio.

Estas inversiones de TI favorecerán la alineación de la estrategia de TI con la estrategia del negocio agregando valor a la organización y favoreciendo el logro de ventajas competitivas sostenibles.

Para lograr este objetivo se debe medir el retorno esperado. Cuanto más enfocadas estén las inversiones en los objetivos estratégicos, más valor obtendrá el negocio. Las decisiones de inversión implican decisiones acerca de cuánto gastar, cuándo gastar y en que gastar así como la priorización, aprobación de proyectos, la justificación técnica de los mismos y la reconciliación de las necesidades de los distintos actores del negocio.

Esto implica una correcta gestión del conocimiento en la organización a través de la adecuada implantación de sus procesos.

La eficiente incorporación, preservación, diseminación y utilización de conocimiento y la experiencia, permitirán alinear el conocimiento estratégico a la estrategia de TI y a la estrategia del negocio de manera de poder tomar buenas decisiones en inversiones de TI que favorecerán el logro de los objetivos del negocio en la organización.

Si analizamos las áreas de enfoque en las cuales se agrupan las actividades de Gobierno de TI y su relación con los procesos de gestión del conocimiento, veremos que en todas las áreas de enfoque ocurren procesos de gestión del conocimiento y que todos los procesos de gestión del conocimiento se relacionan con las áreas de enfoque del Gobierno de TI. Es indispensable el logro de un eficiente Gobierno de TI así como de una eficiente gestión del conocimiento y de un estrecho vínculo entre ambos para el logro de los objetivos organizacionales.

El **alineamiento estratégico** de TI con los objetivos del negocio solo será posible si se gestiona adecuadamente el conocimiento que permita determinar el conocimiento estratégico necesario para lograr los objetivos del negocio.

Solo de esta manera se podrá alinear el conocimiento estratégico con los objetivos de TI y con los objetivos del negocio y asegurar que la inversión en TI de una empresa está acorde con los objetivos estratégicos de la misma, posibilitando la entrega de valor de TI a la organización.

En la **entrega de valor** el Gobierno de TI tiene como objetivo confirmar que TI entrega en todo el ciclo de entrega los beneficios acordados y alineados con la estrategia, concentrándose en la optimización de costos, y demostrando el valor específico de TI.

Para que esto sea posible es necesario que el conocimiento sea gestionado eficientemente, permitiendo la alineación del conocimiento estratégico con los objetivos estratégicos del negocio y con los objetivos estratégicos de TI. Solo de esta manera se podrá garantizar la entrega de valor de TI definida y validada en el área de enfoque de alineamiento estratégico del Gobierno de TI y lograr los objetivos del negocio de la organización.

En relación a las decisiones de **gestión del riesgo** del Gobierno de TI, la adecuada gestión de conocimiento permitirá que se puedan tomar buenas decisiones y se logre prevenir, mitigar o eliminar riesgos que afectan o afectarán a la organización. La gestión del riesgo tiene un estrecho vínculo con la gestión del conocimiento. Si la organización gestiona adecuadamente el conocimiento e incorpora, preserva, disemina y utiliza el conocimiento de manera inteligente, tendrá la información necesaria para poder gestionar adecuadamente el riesgo, previniendo, mitigando o eliminando el mismo de la organización.

Un caso de éxito de la buena gestión del riesgo en función de la buena gestión del conocimiento se da en la organización Chrysler (Basili, V. et al., 1997) donde se muestra un caso de éxito en la implementación de una fábrica de experiencia y la incidencia de la gestión del conocimiento en la gestión del riesgo.

En un período de tres años, un grupo de apoyo en gestión de calidad impulsó un proceso de software de manejo de riesgos, desarrollando proyectos piloto, discutiendo el proceso en grupos de usuarios, remitiéndolo a la administración por aprobación, ofreciendo entrenamiento en cursos adaptados, y usando una base de experiencias en el manejo de riesgos específica y personalizada.

El grupo consideraba a todos los accionistas y sus preocupaciones, diferencias y necesidades anticipando y atendiendo la necesidad de entrenamiento.

Esto permitió que el manejo del riesgo sea ahora aceptado en todo el departamento y aplicado en todos los altos procesos de software estratégicos así como a un creciente número de otros proyectos

de software. Los riesgos son ahora identificados tempranamente y pueden ser mitigados de forma más efectiva.

En relación al área de enfoque de **administración de recursos** del Gobierno de TI, este busca el logro de una óptima inversión y una adecuada administración de los recursos críticos de TI como las aplicaciones, información, infraestructura y personas.

Como vimos anteriormente solo se podrá gobernar exitosamente estos recursos si se gestiona adecuadamente el conocimiento a través de una eficiente incorporación, preservación, diseminación y utilización del mismo en la organización. Luego será necesario la alineación del conocimiento estratégico con la estrategia de la organización y con la estratégica de TI para que la organización esté en condiciones de optimizar sus inversiones y administrar sus recursos críticos de TI en forma eficiente.

La **medición del desempeño** del Gobierno de TI tiene como objetivo el supervisar y dar seguimiento en el desempeño de los procesos, la finalización de proyectos, la estrategia de implementación y la entrega del servicio. En esta área de enfoque se verifica si el desempeño obtenido coincide y cumple con lo definido, planificado y validado en el área de enfoque de alineamiento estratégico del Gobierno de TI, permitiendo de esta manera el logro de los objetivos del negocio y la satisfacción del cliente.

También en esta área de enfoque el conocimiento y su adecuada gestión permitirán que se pueda tener el conocimiento necesario para poder obtener métricas eficientes que sean representativas de la realidad que queremos conocer.

La adecuada gestión del conocimiento a través de la eficiente incorporación, preservación, diseminación y utilización del mismo permitirá saber que medir, como medir y poder interpretar los resultados obtenidos para luego poder evaluarlos y favorecer el alineamiento de la estrategia del negocio, la estrategia de TI y el conocimiento estratégico para el logro de los objetivos de la organización y lograr la satisfacción de los clientes.

Lo que no se puede medir, no se puede administrar y la métrica más importante es el valor que se le brinda al cliente.

De acuerdo a lo presentado y analizado anteriormente podemos apreciar que existe un vínculo muy estrecho entre la Gobernanza de TI y la Gestión del conocimiento.

Cuanto mejor sea la gestión del conocimiento mejor será el Gobierno de TI y cuanto más eficiente sea la Gobernanza de TI se lograra una mejor gestión del conocimiento.

ANEXO XIII – Riesgo desde el punto de vista de la Gestión del Conocimiento

El riesgo se puede mitigar, transferir, aceptar y evitar [1] para lo cual se requiere conciencia de riesgo por parte de los directores superiores de la empresa, entendimiento del apetito del riesgo de la empresa, transparencia sobre los riesgos significativos de la empresa e implementar las responsabilidades de la administración de riesgos dentro de la organización.

Se definen así las siguientes 4 variables a tener en cuenta en la gestión del riesgo:

- 1) Grado de Conciencia de riesgo por parte de los directores de la empresa.
- 2) Entendimiento del apetito de riesgo de la empresa.
- 3) Transparencia sobre los riesgos significativos de la empresa.
- 4) Nivel de compromiso de la alta dirección en la implementación de las responsabilidades de la administración de riesgos dentro de la organización.

Contemplando las variables anteriores, se identifican las siguientes variables con una visión desde la gestión del conocimiento, con lo que tenemos:

- Variable de riesgo 1: Grado de definición de conocimientos, habilidades y capacidades alineados a la estrategia del negocio. Definición de una base de conocimiento que cumpla con los objetivos organizacionales.

El hecho de que las Pymes en general no definan formalmente sus conocimientos, habilidades y capacidades necesarias para cumplir con la estrategia de negocios definida, hace que estas sean más vulnerables a los riesgos de no contar con las capacidades, conocimiento, experiencia, habilidades y competencias necesarias para cumplir con las necesidades del negocio.

A su vez la creación de una base de conocimiento que esté de acuerdo a las necesidades de diversos factores como la tecnología, los mercados, los productos y los procesos necesarios para el negocio, minimizara los riesgos de fracaso en el cumplimiento de la estrategia favoreciendo el logro de los objetivos organizacionales.

- Variable de riesgo 2: Grado de identificación de conocimientos que son estratégicos para la organización. Implica la identificación del conocimiento que existe en la organización y las brechas de conocimiento entre este y el conocimiento estratégico.

La no identificación de los conocimientos estratégicos para la organización implica un riesgo en el logro de los objetivos del negocio así como un riesgo de oportunidad. Si no se conocen los conocimientos que existen en la organización y no se identifica el conocimiento estratégico que necesita la organización para cumplir con sus objetivos del negocio, no se podrá conocer las capacidades de los recursos humanos con los que cuenta la organización y se pierde la oportunidad de capacitar a sus recursos humanos para que apoyen el logro de los objetivos del negocio y encuentren oportunidades y ventajas competitivas sostenibles.

Al no poder identificar los conocimientos, habilidades y experiencias existentes en la organización y en consecuencia la eficiencia y carencia en los conocimientos y experiencia, se presenta el riesgo de que la organización no pueda conocer hasta qué punto es capaz de hacer determinadas acciones para favorecer el logro de los objetivos del negocio. De esta manera la organización no podrá tener claro que es lo que puede y que es lo que debe hacer, dificultando de esta manera el logro de los objetivos organizacionales.

- Variable de riesgo 3: Grado de incorporación del conocimiento y la experiencia en la organización con el objetivo de disminuir o eliminar las brechas de conocimiento identificadas en la variable de riesgo 2.

La falta de incorporación del conocimiento y la experiencia en la organización, ya sea a través de fuentes externas a la misma o mediante la creación y desarrollo de conocimientos generados internamente, pone en riesgo a la misma y la hace vulnerable a no poder alcanzar sus objetivos del negocio.

- Variable de riesgo 4: Grado de preservación del conocimiento en la organización con el objetivo de mantener el conocimiento organizacional y asegurar la continuidad del mismo.

La no preservación del conocimiento en la organización implica el riesgo de no poder avanzar, es decir tener que “reinventar la rueda” cada vez que se nos presenta un problema similar, no poder aprovechar y re utilizar lo aprendido en una situación anterior perdiendo tiempo dinero y eficiencia. Esto se da ante la falta de formalización, codificación, organización y almacenamiento en algún medio del conocimiento y la no retención de los talentos poseedores de conocimiento tácito.

- Variable de riesgo 5: Grado de diseminación del conocimiento en la organización con el objetivo de distribuir y compartir el conocimiento a través de los diferentes niveles organizacionales a quienes deben recibirlo para luego difundirlo a la organización a través de canales claramente definidos.

Si el conocimiento no es distribuido y compartido, se presenta el riesgo que no llegue a quienes requieran del mismo para contribuir al logro de los objetivos del negocio en la organización. Esto desfavorece la culturización de la gestión del conocimiento en la organización poniendo en riesgo a los objetivos del negocio. La definición de los responsables de distribuir el conocimiento, el tener claro los niveles y formas de distribución y recepción del conocimiento así como el acceso al mismo serán factores determinantes del éxito de la Gestión del conocimiento en la organización.

- Variable de riesgo 6: Grado de aplicación y utilización del conocimiento en la organización. Implica el nivel de aplicación y utilización del conocimiento creado o adquirido de las mejores prácticas y lecciones aprendidas.

La no utilización del conocimiento creado o adquirido a través de los repositorios de las lecciones aprendidas y mejores prácticas dejara vulnerable a la organización de no poder aprender de la experiencia, y en consecuencia esta perderá oportunidades de mejora y aumentaran los riesgos de no satisfacción de los objetivos organizacionales.

- Variable de riesgo 7: Existencia de innovación: La innovación implica generar oportunidades de mejora.

Se identifica la existencia de un riesgo importante en la falta de innovación ya que se pierde la oportunidad de identificar e implementar una ventaja competitiva sostenible a las necesidades del negocio.

Anexo XIV – Matrices del Marco de Gestión del Riesgo basado en la Gestión del Conocimiento

Dominio: Proceso Gobierno del Riesgo (RG)

Gestión del Riesgo Proceso Gobierno del Riesgo (RG)	Gestión del Conocimiento aplicado al Proceso Gobierno del Riesgo (RG)	Implementación de la Gestión del Conocimiento aplicado al Proceso Gobierno del Riesgo (RG)
RG1: Establece y mantiene una visión de riesgo común.	Gestionando el conocimiento sobre la situación de cada área del negocio y la de su cartera de proyectos a nivel organizacional y estableciendo métricas eficientes que sean claras para que todos los responsables de las mismas puedan conocer y minimizar en todo momento el riesgo de su área a través de un alineamiento de sus objetivos con los objetivos del negocio, minimizando de esta manera el riesgo de toda la organización. Se generara una cultura organizacional sobre la gestión del conocimiento.	Se implementa una base de conocimiento (KDBMS) que tenga registro de los objetivos organizacionales a realizar (apetito al riesgo) y las acciones a ejecutar por cada área del negocio para el logro de estos objetivos. Se deberá capacitar y formar a los gerentes de cada área y a sus recursos humanos para que puedan registrar y actualizar estas acciones con el apoyo y autorización de la dirección general.
RG1.1 Desarrollar en una empresa el marco específico de gestión de riesgos de TI	Gestionando el conocimiento a través de la identificación, registro y análisis de las variables más significativas del negocio. Identificando los principales puntos de soporte de TI que generan valor al negocio para poner especial énfasis en el análisis y tolerancia al riesgo de los mismos.	A través de mapas de conocimiento donde se identifiquen y vinculen eventos relacionados con TI que aportan valor al negocio ponderados según categorías de riesgo para poder identificar y minimizar posibles riesgos en cascada y añadirle valor al negocio.
RG1.2 Proponer los umbrales de tolerancia de riesgos de TI	Gestionando el Conocimiento de los procesos fundamentales del negocio, se podrán definir, medir y administrar los niveles de riesgo de estos, permitiendo generar alertas en caso de que se excedan los mismos, favoreciendo de esta manera la mitigación de los riesgos del negocio.	A través de bases de conocimiento (KDBMS) y por medio de mapas de conocimiento que permitan ingresar y actualizar umbrales de riesgo para cada proyecto en medidas similares a los objetivos del negocio.

<p>RG1.3 Aprobar la tolerancia al riesgo</p>	<p>Al conocer los umbrales de tolerancia al riesgo para los procesos fundamentales del negocio, se podrá evaluar la posibilidad de la aprobación o modificación de estos umbrales o de alguno de estos en alguna unidad del negocio, frente a un riesgo aceptable de la empresa y los niveles de oportunidad para mejorar la relación riesgo/retorno.</p>	<p>Por medio de los mapas y bases de conocimiento (KDBMS) que permitan actualizar los umbrales del riesgo de cada área del negocio en relación a las oportunidades que se presenten para los eventos (internos o externos) que ameriten la modificación de los umbrales del riesgo y el logro de los objetivos clave para la relación riesgo/retorno.</p>
<p>RG1.4 Alinear la política de riesgos de TI</p>	<p>Gestionando el conocimiento a nivel de toda la organización y codificando el apetito por el riesgo y la tolerancia de cada área del negocio en la política de riesgos, de manera que esta esté alineada con los objetivos de la organización.</p>	<p>A través de bases de conocimiento y grupo de expertos que permitan codificar el apetito de riesgo y la tolerancia de cada área de manera que estén alineados con los objetivos del negocio, aportando valor a la misma.</p>
<p>RG1.5 Promover los riesgos de TI – cultura consciente</p>	<p>Gestionando el conocimiento a través de la formación y capacitación del personal responsable en la gestión del riesgo, para que la política de riesgo sea transmitida a toda la organización y logre el involucramiento de todos los recursos humanos y para que cada uno desde su lugar favorezca la gestión del riesgo, alineando sus estrategias según la identificación proactiva de los riesgos de TI, las oportunidades y los impactos potenciales, retroalimentando la política de riesgo y favoreciendo al logro de los objetivos organizacionales.</p>	<p>Por medio de la utilización de conocimiento sobre las distintas acciones y buenas prácticas de la gestión del riesgo en las distintas áreas del negocio, promoviendo una cultura de riesgos responsable a través de sus responsables en búsqueda de una adecuada política de riesgos organizacional. A través de la Gestión del conocimiento por medio de bases de conocimiento (KDBMS), mapas y técnicas de GC donde a través de la formación y capacitación del personal sobre la política de riesgo organizacional y como transmitirla en todas las áreas de valor para el negocio. Comunicar y aplicar las buenas practicas a seguir para cumplir con este objetivo.</p>

<p>RG1.6 Promover una comunicación efectiva de los riesgos de TI</p>	<p>A través del conocimiento por parte de los recursos humanos de las políticas de gestión del riesgo de TI, se podrá establecer un plan de comunicación de riesgos para cumplir efectivamente con estas políticas. Se podrán tomar decisiones de negocio a través del conocimiento de los responsables, controles, amenazas e impacto del riesgo en cada área del negocio. Es a través de las herramientas y técnicas de Gestión del conocimiento que se podrán tomar decisiones conjuntas entre los responsables de TI y los directores del negocio, favoreciendo la comunicación efectiva de los riesgos de TI en toda la organización, priorizando riesgos según el impacto de los mismos al negocio, comprendiendo la importancia de minimizar riesgos y la asignación de recursos para esta actividad, alineando la política de riesgos con los objetivos del negocio.</p>	<p>A través de una base de conocimiento (KDBMS) donde accedan los directores de las distintas áreas, directores de TI, la dirección general y los recursos humanos adecuados según sus roles, responsabilidades y funciones, en donde estos puedan a través de mapas y redes de conocimiento acceder, intercambiar y actualizar en conjunto el conocimiento fundamental sobre la efectiva gestión del riesgo de TI a toda la organización de TI, lo que permitirá tomar mejores decisiones para el negocio.</p>
<p>RG2: Integrar con ERM</p>	<p>Gestionando el conocimiento a través del acceso del responsable de TI y los responsables de los distintos departamentos del negocio en todas sus áreas a una base de conocimiento común donde se registre, actualice y alinee la estrategia de riesgos de TI y operaciones de TI y con las decisiones estratégicas a nivel del negocio.</p>	<p>A través de una base de datos de conocimiento (KDBMS) y de mapas de conocimiento donde a través de una capacitación de los recursos humanos responsables, por medio de técnicas como el coaching y el mentoring, estos registren actualicen y alineen la estrategia de riesgos de TI y sus operaciones con la estrategia de riesgos del negocio.</p>

<p>RG2.1 Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa</p>	<p>Gestionando el conocimiento a través de la creación y difusión de una conciencia y cultura de Gestión del conocimiento en toda la organización, en la que todos participen según sus roles y responsabilidades; creando, registrando, transfiriendo, usando y midiendo el conocimiento para cumplir con las métricas de la gestión del riesgo definidas, evaluando y definiendo el nivel de criticidad del riesgo en función de la relación riesgo-recompensa y la relación riesgo-retorno, favoreciendo de esta manera la gestión de riesgos de TI en toda la organización.</p>	<p>A través de una base de datos de conocimiento (KDBMS) auditable, en la que los recursos humanos según su rol, responsabilidades y departamento al que pertenecen definidos a través de mapas de conocimiento, registren y actualicen (a través de una capacitación por, coaching y mentoring), los conocimientos necesarios para gestionar el riesgo, de acuerdo a la criticidad del mismo, de forma que este se alinee y cumpla con el plan de riesgos de TI definidos en la organización.</p>
<p>RG2.2 Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial.</p>	<p>Gestionando el conocimiento, de manera que el director de TI, los directores de cada área y la dirección general accedan, interactúen y actualicen a través de una base de conocimiento común, el conocimiento y los recursos necesarios, de forma que se pueda alinear la estrategia de riesgos de TI y sus procesos de protección y mantenimiento del riesgo con el proceso del negocio y la estrategia de riesgo empresarial, estableciendo escalas de clasificación, categorías de control y jerarquías de riesgo que cumplan con los objetivos del negocio.</p>	<p>A través de una base de conocimiento (KDBMS) y mapas de conocimiento, donde los directores de TI y los directores de las distintas áreas accedan, registren, generen, usen y transfieran conocimiento que permita su capacitación y la definición en conjunto de escalas, categorías y jerarquías de riesgo que posibiliten la coordinación de la estrategia de riesgos de TI y la estrategia de riesgo empresarial favoreciendo el logro de los objetivos del negocio.</p>

<p>RG2.3 Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa.</p>	<p>Gestionando el conocimiento de manera que el director de TI pueda identificar a través de una base de conocimiento común junto al director general y los directores de cada departamento, cuáles son las prácticas de riesgo de la empresa y generar o adquirir, transmitir y usar el conocimiento necesario para alinear estas con las prácticas de TI. A su vez la dirección general podrá entender el contexto de negocio de TI e identificar, regular y gestionar los riesgos de TI y retroalimentar estos con las expectativas de la empresa en gestión de riesgos.</p>	<p>A través de una base de conocimiento (KDBMS) común y mapas de conocimiento, donde el director de TI, pueda identificar y adquirir el conocimiento necesario acerca de las prácticas de riesgo de la empresa para poder alinear estas a las prácticas de TI y en conjunto poder usar y transmitir una cultura de riesgo y gestión del conocimiento a toda la organización. Se capacitara a los recursos humanos a través de técnicas como coaching y mentoring para que puedan realizar esta tarea en forma eficiente.</p>
--	---	--

<p>RG2.4 Proporcionar recursos adecuados para la gestión de riesgos.</p>	<p>Gestionando el conocimiento a través de la adquisición e incorporación de recursos humanos y la capacitación integral de estos a lo largo de toda la organización para favorecer su eficiencia en la gestión de riesgos. El acceso y actualización de los distintos riesgos y sus criticidades según los objetivos del negocio a través de una base de conocimiento común (KDBMS) permitirá identificar, capacitar y adquirir los recursos humanos adecuados, personas y habilidades, establecer como especificar los conocimientos de gestión del riesgo de los administradores y el personal de desarrollo y mantenimiento, los procesos y procedimientos documentados para la gestión de los riesgos de TI, sistemas de información y base de datos para cuestiones de gestión de TI, presupuesto y otros recursos para la respuesta específica de actividades de riesgo, expectativas de los reguladores y los auditores externos para poder cumplir con estos objetivos, minimizando los riesgos y descubriendo y aprovechando nuevas oportunidades de mejora y de entrega de valor al negocio.</p>	<p>Por medio de una base de conocimiento común (KDBMS) y mapas de conocimiento que establezcan relaciones de conocimiento entre los distintos roles y responsables, para de esta manera posibilitar la formación y/o adquisición de los recursos humanos a través de técnicas como el coaching, mentoring y grupos expertos. De esta manera se podrán establecer sistemas de información, expectativas de los reguladores y auditores externos y presupuestos adecuados para favorecer la gestión de riesgos desde TI al negocio para el logro de los objetivos del mismo.</p>
--	---	--

<p>RG2.5 Garantizar el aseguramiento independiente sobre la gestión de riesgos</p>	<p>Gestionando el conocimiento por medio de una base de conocimiento común (KDBMS) a través de la cual el director de TI acceda, evalúe, registre y actualice los planes de gestión del riesgo de TI, el desempeño de las principales prácticas para su gestión y verifique si el riesgo se gestiona de acuerdo con el apetito de riesgo y la tolerancia adecuados para el cumplimiento con la Gestión del riesgo del negocio. Estos elementos a su vez se irán identificando, incorporando y actualizando a través del director general en la base de conocimiento. Tanto el director de TI como el director general serán formados para este fin.</p>	<p>Por medio de una base de conocimiento común (KDBMS) y mapas de conocimiento que establezcan relaciones de conocimiento entre los distintos roles y responsables capacitando a los recursos humanos, director general y director de TI a través de coaching, mentoring y grupos expertos, para asegurar la independencia de la Gestión de riesgos de TI en el cumplimiento de la gestión de riesgos de la organización.</p>
<p>RG3 Toma de decisiones consciente del riesgo de negocio</p>	<p>Gestionando el conocimiento por medio de una base de conocimiento común (KDBMS) a través de la que el director general, directores de área y director de TI accedan, evalúen, registren y actualicen los planes de gestión del riesgo del negocio y de TI respectivamente, tomando muy en cuenta la importancia de TI en la gestión del riesgo del negocio y alineando las prácticas de Gestión del riesgo de TI a la Gestión de Riesgos del negocio, tomando decisiones en forma conjunta, favoreciendo el logro de los objetivos del negocio. Los responsables serán formados para poder cumplir con este objetivo.</p>	<p>A través de una base de conocimiento común (KDBMS) y mapas de conocimiento que establezcan relaciones de conocimiento entre los directores generales, directores de área y director de TI, para que a través de la capacitación por medio de grupos expertos, coaching y mentoring puedan identificar, adquirir, transferir y usar el conocimiento para poder tomar decisiones en conjunto y alinear la Gestión de riesgos de TI con la Gestión de riesgos del negocio.</p>

<p>RG3.1 Ganancia de la gestión de compra para el enfoque de análisis de riesgos.</p>	<p>Gestionando el conocimiento a través de la formación de los recursos humanos para que comprendan la importancia de la gestión de riesgos de TI en la gestión de los riesgos del negocio y como a través de una eficiente gestión de riesgos se pueden tomar buenas decisiones. Por medio de una base de conocimiento común (KDBMS) en la que se defina, registre, transfiera y use la calidad que se debe esperar de la toma de decisiones, cómo interpretar los informes de análisis de riesgos y definiciones de términos clave, de manera que todos puedan tener claro cómo medir el riesgo e identificar las brechas existentes con el riesgo empresarial para reducirlas y favorecer los objetivos del negocio.</p>	<p>Por medio de técnicas y herramientas como grupos expertos, coaching, mentoring para capacitar a los recursos humanos y a través de una base de conocimiento común (KDBMS) y mapas de conocimiento entre los recursos humanos responsables de la gestión del riesgo de TI y de la gestión del riesgo del negocio para poder tomar decisiones en conjunto, comprender la importancia de la gestión de los riesgos de TI para los riesgos del negocio y favorecer los objetivos del mismo.</p>
<p>RG3.2 Aprobar el análisis de riesgos de TI</p>	<p>Gestionando el conocimiento a través de una base común de conocimiento en la que los directores de las distintas áreas de la organización por medio de capacitación y cultura organizacional, identifiquen, registren, transfieran y usen los riesgos inherentes de su área para el negocio y donde el director de TI pueda evaluar los riesgos de este departamento y alinearlos mediante la aprobación del director general, a los riesgos del negocio.</p>	<p>A través de una base común de conocimiento (KDBMS) para que los directores de las distintas áreas identifiquen, registren, transfieran y usen el conocimiento en un repositorio común. A través de herramientas y técnicas como el coaching, mentoring y grupos expertos, para capacitar a los directores de las distintas áreas para el logro de una cultura organizacional de gestión del riesgo a través de la gestión del conocimiento.</p>

<p>RG3.3 Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio</p>	<p>Gestionando el conocimiento a través de una base de conocimiento común (KDBMS) en la que el director de TI registre, actualice, transfiera y use el conocimiento sobre el riesgo de TI para el negocio, de forma que el director general pueda incorporar estos conocimientos en la gestión de riesgos del negocio y considerarlos para la toma de decisiones estratégicas del mismo. Esto permite la toma de decisiones en conjunto lo cual favorece los objetivos estratégicos de la organización. Esto será más efectivo en la medida que se gestione el conocimiento a través de una capacitación de los riesgos de TI y del negocio así como una culturización para la toma de decisiones en conjunto.</p>	<p>A través de una base de conocimiento común (KDBMS) y de mapas del conocimiento en las que se establezcan relaciones sobre la incidencia de los riesgos de TI en el negocio.</p> <p>Por medio de la adquisición y/o capacitación de los recursos humanos (director general y director de TI) en los conocimientos necesarios para gestionar los riesgos de TI y del negocio, generando una cultura de toma de decisiones conjunta que considere los riesgos de TI en las decisiones estratégicas del negocio.</p>
--	--	---

RG3.4 Aceptar los riesgos de TI	<p>Gestionando el conocimiento en la organización de manera que se establezca una cultura a todo nivel sobre la importancia de los riesgos de TI para el riesgo del negocio. Formando a los recursos humanos responsables, director general de cada área del negocio para que a través de una base de conocimiento común identifiquen, definan, accedan , actualicen y usen los umbrales de tolerancia al riesgo y puedan en conjunto establecer si aceptan el nivel de riesgo de exposición, las opciones de respuesta ante el riesgo y el costo - beneficio de la agregación de riesgos así como el presupuesto de riesgos conocidos para evaluar el permitir riesgos desconocidos y registrar a través de documentos los criterios de consideración del riesgo para que sea transversal a toda la organización de acuerdo a sus políticas y procedimientos.</p>	<p>Por medio de una base de conocimiento común (KDBMS) y redes de conocimiento que establezcan relaciones entre los directores de cada área para que puedan gestionar el riesgo en conjunto de acuerdo a la responsabilidad de cada recurso humano. Por medio de la adquisición y/o capacitación de los recursos humanos (director general, director de TI y directores de cada área del negocio) a través de herramientas como grupos expertos, coaching y mentoring en los conocimientos necesarios para aceptar y gestionar los riesgos de TI y del negocio, que permita generar una cultura transversal a toda la organización de acuerdo a sus políticas y procedimientos.</p>
---------------------------------	--	---

<p>RG3.5 Priorizar actividades de respuesta de riesgos de TI</p>	<p>Gestionando el conocimiento en la organización de manera que el director de TI con el apoyo del director general pueda identificar, adquirir, transferir, registrar y usar el conocimiento a través de una base de conocimiento común (KDBMS) donde pueda examinar, registrar y priorizar la cartera de actividades de TI de respuesta al riesgo según sea el impacto probable de estas sobre la reducción del riesgo global. Esto favorece la toma de decisiones conjuntas para el logro de los objetivos del negocio. Definiendo y registrando métricas en la base de conocimiento común que permitan medir el grado de cumplimiento de las actividades de TI, los controles, la capacidad y los recursos, y registrando la razón en el caso de que se sobrepase o caiga por debajo del apetito y tolerancia de riesgo del negocio, se podrá gestionar el conocimiento de manera de priorizar y hacer énfasis en proyectos que permitan una mejor gestión del riesgo de acuerdo al apetito y tolerancia al riesgo del negocio, favoreciendo los objetivos de la organización.</p>	<p>A través de una base de conocimiento común (KDBMS) y mapas de redes que establezcan relaciones de conocimiento entre los recursos humanos responsables como ser el director general y el director de TI, capacitando a estos a través de grupos expertos, coaching y mentoring para que puedan priorizar las actividades de respuesta de riesgos de TI para que se alineen a la gestión de riesgos del negocio.</p>
--	--	--

RG1.1 Desarrolla en una empresa el marco específico de gestión de riesgos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional	Realidad virtual. Sistemas expertos. Charlas informales. Bases de conocimiento. E-learning. Clasificación. Clustering	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG1.2 Proponer los umbrales de tolerancia de riesgos de TI	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional	Realidad virtual. Sistemas expertos. Charlas informales. Bases de conocimiento. Clasificación. Mentoring Coaching	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG1.3 Aprobar la tolerancia al riesgo	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional	Realidad virtual. Sistemas expertos. Charlas informales. Bases de conocimiento. Clasificación. Mentoring Coaching	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG1.4 Alinear la política de riesgos de TI	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Comunidades de práctica y grupos expertos. Redes Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Memoria organizacional	Sistemas expertos. Charlas informales. Bases de conocimiento. Clasificación. Clustering	Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG1.5 Promover los riesgos de TI – cultura consciente	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Redes. Mapas. Lecciones aprendidas. Mejores prácticas. Benchmarking Memoria organizacional	Sistemas expertos. Charlas informales. Bases de conocimiento. Clasificación. Clustering	Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG1.6 Promover una comunicación efectiva de los riesgos de TI	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Redes. Mapas. Lecciones aprendidas. Mejores prácticas. Memoria organizacional	Videoconferencia Realidad virtual. Sistemas expertos. Charlas informales. Bases de conocimiento. Clasificación. Mentoring Coaching Clustering	Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG2.1 Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Accesibilidad. Diseño del área de trabajo. Benchmarking . Fusión o Adquisición. Redes. Mapas. Lecciones aprendidas. Mejores prácticas. Memoria organizacional	Realidad virtual. Sistemas expertos. Charlas informales. Bases de conocimiento. Clasificación. Mentoring Coaching Clustering	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG2.2 Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial.	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Grupos Expertos Benchmarking Fusión o Adquisición. Redes. Mapas. Patentes. Lecciones aprendidas. Mejores prácticas. Grupos Expertos Memoria organizacional	Realidad virtual. Sistemas expertos. Charlas informales. Bases de conocimiento. Clasificación. Mentoring Coaching Clustering	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG2.3 Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa.	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Grupos Expertos Benchmarking Fusión o Adquisición. Redes. Mapas. Lecciones aprendidas. Mejores prácticas. Grupos Expertos Memoria organizacional	Videoconferencia Realidad virtual. Sistemas expertos. Charlas informales. Bases de conocimiento. Clasificación. Mentoring Coaching Clustering	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG2.4 Proporcionar recursos adecuados para la gestión de riesgos.	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	<p>Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.</p>	<p>Grupos Expertos</p> <p>Benchmarking</p> <p>Fusión o Adquisición.</p> <p>Redes.</p> <p>Mapas.</p> <p>Lecciones aprendidas.</p> <p>Mejores prácticas.</p> <p>Grupos Expertos</p> <p>Memoria organizacional.</p>	<p>Videoconferencia</p> <p>Realidad virtual.</p> <p>Sistemas expertos.</p> <p>Charlas informales.</p> <p>Bases de conocimiento.</p> <p>Clasificación.</p> <p>Mentoring</p> <p>Coaching</p> <p>Clustering</p>	<p>Recursos económicos.</p> <p>Tiempo.</p> <p>Capacitación.</p> <p>Recursos Humanos.</p> <p>Marcos de Buenas prácticas.</p> <p>Cultura organizacional.</p> <p>CKO (En caso de existir este rol).</p> <p>Compromiso de la alta gerencia.</p>

RG2.5 Garantizar el aseguramiento independiente sobre la gestión de riesgos	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación de los directivos, registro, acceso y distribución del conocimiento en la KDBMS.	Grupos Expertos Fusión o Adquisición. Redes. Mapas. Lecciones aprendidas. Mejores prácticas. Memoria organizacional	Charlas informales. Bases de conocimiento. Clasificación. Mentoring Coaching Clustering	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG3.1 Ganancia de la gestión de compra para el enfoque de análisis de riesgos	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación del personal, registro, acceso y distribución del conocimiento en la KDBMS por el personal adecuado.	Grupos Expertos Benchmarking. Fusión o Adquisición. Redes. Mapas. Lecciones aprendidas. Mejores prácticas. Memoria organizacional.	Charlas informales. Bases de conocimiento. Clasificación. Mentoring Coaching Clustering	Recursos económicos. Tiempo. Capacitación. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG3.2 Aprobar el análisis de riesgos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y a través de la cultura organizacional lograr la formación de los directores, en registro, acceso y distribución del conocimiento.	Grupos Expertos Mapas. Lecciones aprendidas. Mejores prácticas. Memoria organizacional.	Charlas informales. Bases de conocimiento. Mentoring Coaching	Recursos económicos. Tiempo. Capacitación. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG3.3 Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación de los directores y director de TI, para el uso del conocimiento sobre riesgo en TI de la KDBMS.	Grupos Expertos Mapas. Lecciones aprendidas. Mejores prácticas. Memoria organizacional.	Charlas informales. Bases de conocimiento. Mentoring Coaching	Recursos económicos. Tiempo. Capacitación. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG3.4 Aceptar los riesgos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y formación de los directivos de cada área, directores de la organización y de TI, en el manejo de información de riesgos y su costo-beneficio para la aceptación de riesgos, en el registro, acceso y distribución del conocimiento en la KDBMS.	Grupos Expertos Redes. Mapas. Lecciones aprendidas. Mejores prácticas. Memoria organizacional.	Sistemas expertos. Charlas informales. Bases de conocimiento. Mentoring Coaching	Recursos económicos. Tiempo. Capacitación. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RG3.5 Priorizar actividades de respuesta de riesgos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en el uso del conocimiento para priorizar las respuestas de riesgos en TI.	Grupos Expertos Mapas. Lecciones aprendidas. Mejores prácticas. Memoria organizacional.	Sistemas expertos. Charlas informales. Bases de conocimiento. Mentoring Coaching	Recursos económicos. Capacitación. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

Cuadros RACI

RG1 – Establece y Mantiene una Visión de Riesgo Común

Funciones Actividades principales	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
	RG1.1 Desarrolla en una empresa el marco específico de gestión de riesgos TI	C	A	R	R	R	R	I	C	C	C	C
RG1.2 Proponer los umbrales de tolerancia de riesgo de TI	I	I	A	C	R	C	I	I	C	C		C
RG1.3 Aprobar la tolerancia al riesgo	A	C	R	C	C	C	C	C	C	C	C	C
RG1.4 Alinear la política de riesgos de TI	C	A	R	C	R	R	C	R	R	R	R	C
RG1.5 Promover los riesgos de TI – cultura consciente.	A	R	R	R	R	R	R	R	R	R	R	R
RG1.6 Promover una comunicación efectiva de los	R	R	A	R	R	R	R	R	R	R	R	R

Nota : R – Responsable A – Responsable (autoriza) C – Consultado I - Informado

RG2 – Integrar con ERM

Funciones Actividades principales	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
	RG2.1 Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	A	R	R	R	R	R	I	I	I	C	C
RG2.2 Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial	A	R	C	R	R	C	C	R	C	C	C	I
RG2.3 Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa			A	R	R	C	I	C	C	C	C	C
RG2.4 Proporcionar recursos adecuados para la gestión de riesgos	A	R	C	C	R	C	I	R	R	C	C	I
RG2.5 Garantizar el aseguramiento independiente sobre la gestión de riesgos	I	A	R	R	R	C	C	C	C	C	C	C

Nota : R – Responsable A – Responsable (autoriza) C – Consultado I - Informado

RG3 – Toma de decisiones consciente del riesgo de negocio

Funciones	Actividades principales											
	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
RG3.1 Ganancia de la gestión de compra para el enfoque de análisis de riesgos		C	A	R	R	C	C	C	C	R	C	C
RG3.2 Aprobar el análisis de riesgos de TI		I	R	R	R	C	A	R	R	I	I	I
RG3.3 Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	I	C	C	C	A	C	C	C	C	R	C	R
RG3.4 Aceptar los riesgos de TI	I	I	A	C	R	C	R	R	R	C		I
RG3.5 Priorizar actividades de respuesta de riesgos de TI		I	A	C	R	I	C	R	R	R		C

Nota : **R** – Responsable **A** – Responsable (autoriza) **C** – Consultado **I** - Informado

Dominio: Proceso Evaluación del Riesgo (RE)

Gestión del Riesgo Proceso Evaluación del Riesgo (RE)	Gestión del Conocimiento aplicado al Proceso Evaluación del Riesgo (RE)	Implementación de la Gestión del Conocimiento aplicado al Proceso Evaluación del Riesgo (RE)
RE1: Recopilar datos	A través de la definición e implementación de una estrategia de gestión del conocimiento, se podrá identificar, adquirir y retener los datos, información y conocimiento relevante para la mejora en la gestión del riesgo. La estrategia debe definir los procesos, flujos de trabajo y medios internos y externos a la organización, los que permitirán actualizar la base de conocimiento de la misma, pudiendo recopilar datos de una forma más eficiente y logrando de esta manera una mejora en la gestión del riesgo.	Por medio de la formación y capacitación de los recursos humanos en las diferentes áreas de la organización a través de herramientas y técnicas de Gestión del Conocimiento como sistemas y grupos de expertos, mentoring, coaching, lecciones aprendidas y mejores prácticas, donde a través del compromiso y apoyo de la dirección y la culturización del personal en la Gestión del Conocimiento, se pueda a través de un repositorio único, categorizado, que brinda a los responsables de cada área de la organización una visión común sobre el riesgo, facilitando la toma de decisiones a través de la recopilación eficiente de datos, en los conocimientos necesarios para lograr una recopilación de datos eficiente donde la dirección general, el director de TI y el director financiero puedan implementar la estrategia de Gestión de Conocimiento en conjunto.

<p>RE1.1 Establecer y mantener un modelo para la recolección de datos</p>	<p>Gestionando el conocimiento de manera que exista un compromiso de la dirección de la organización y a través de la capacitación de los recursos humanos implicados en la recolección de datos, para que la estrategia de la misma se alinee con el conocimiento identificado, adquirido, retenido y desarrollado en las distintas etapas de Gestión del conocimiento mediante una base de conocimiento de riesgos común a los responsables de las distintas áreas de la organización por medio por ejemplo de una memoria organizacional que pueda ir alimentando y desarrollando la estrategia de Gestión de conocimiento para poder recolectar datos de una forma más eficiente.</p> <p>Estableciendo una estrategia de gestión del conocimiento que facilite la accesibilidad a los datos de riesgo, así como su mantenibilidad, minimizando los tiempos de respuesta y correspondiente costo económico.</p>	<p>Aplicando las herramientas y técnicas de gestión del conocimiento, que permiten identificar, adquirir, retener y desarrollar el conocimiento organizacional, como ser registro de lecciones aprendidas, charlas informales, relevamiento de información del personal experimentado, capacitación y formación interna y externa, mentoring y coaching. Formando un CMS (repositorio de gestión del conocimiento), que permitirá acceder a la información según distintas clasificaciones de riesgo, facilitando su acceso y tiempo de respuesta.</p> <p>Por medio de técnicas de gestión del conocimiento como benchmarking y charlas con expertos, se identifica, clasifica e integra en la base de conocimiento la información del entorno de la empresa, permitiendo así incluir en la base de conocimiento información que ayude en la toma de decisiones, para la prevención de riesgos en TI a los responsables de cada área.</p>
<p>RE1.2 Recopilar datos sobre el entorno externo</p>	<p>Aplicando técnicas de gestión del conocimiento se identifica, adquiere, retiene y distribuye conocimiento sobre el entorno operativo y competitivo de la empresa que puede influir en la mejor gestión de TI, permitiendo nutrir la base de conocimiento con información histórica de la empresa y de su entorno, intercambiando dicho conocimiento se contará con experiencias propias y de terceros, lo cual permitirá mejores resultados en la toma de decisiones en la evaluación y gestión del riesgo en TI.</p>	<p>Por medio de técnicas de gestión del conocimiento como benchmarking y charlas con expertos se identifica, adquiere, clasifica, retiene, integra y distribuye en la base de conocimiento la información del entorno de la empresa, permitiendo así incluir en la base de conocimiento información que ayude en la evaluación del riesgo y toma de decisiones, para la prevención de riesgos a los responsables de cada área.</p>

<p>RE1.3 Recopilar datos sobre eventos de riesgo</p>	<p>Junto a los directivos de la organización y responsables de TI, aplicando técnicas y herramientas de gestión del conocimiento se identifican y registran en una base de conocimiento común los datos asociados a proyectos, programas, servicios existentes y futuros, etc. que pueden generar eventos de riesgo, lo cual brindará una visión más íntegra de los riesgos reales de TI en el negocio permitiendo mejores resultados en la toma de decisiones, evaluación y gestión del riesgo de TI.</p>	<p>Por medio de técnicas y herramientas de Gestión del Conocimiento como coaching, comunidades de prácticas, charlas con expertos y charlas informales con los responsables de TI y directivos de la organización, se integra en una base de conocimiento común información sobre proyectos, programas, servicios e incidentes. De esta manera se podrá contar con una visión general y real de los riesgos actuales y futuros, lo que permitirá mejorar la gestión de riesgos de TI.</p>
<p>RE1.4 Identificar factores de riesgo</p>	<p>Incrementando el conocimiento disponible en la CMS con la codificación de la información relacionada a los factores de riesgo asociado a los riesgos identificados, vinculando los factores de riesgo con la frecuencia y magnitud de los riesgos. Por medio de la externalización y socialización del conocimiento de los recursos humanos, se internaliza y combina el conocimiento generando nuevo conocimiento y conciencia sobre el riesgo y los factores vinculados.</p>	<p>Recopilando información sobre el vínculo de factores de riesgo asociados a riesgos existentes o similares, aplicando técnicas de gestión del conocimiento como ser charlas informales, asesoramiento con expertos, métodos de clasificación y clustering para agrupar riesgos según un mismo factor de riesgo y lecciones aprendidas. Realizando este relevamiento de información con el compromiso de los recursos humanos de la empresa, capacitando a estos en gestión del riesgo, aumentando así su conocimiento y conciencia de riesgo.</p>

RE2: Análisis de Riesgo	Con el compromiso de los directivos, CIO y responsables del riesgo, organizando la información de riesgos de acuerdo a su frecuencia, magnitud y factores asociados, así como sus posibles respuestas. Por medio de la gestión del conocimiento, se podrá analizar el riesgo y determinar los límites, recursos necesarios para asumir el riesgo definido, así como ponderar y determinar las respuestas ante un evento de riesgo.	Por medio del uso de mapas de conocimiento que nos permiten visualizar los riesgos a nivel de organización, diseño de grupos de trabajo para organizar los recursos de forma óptima según las decisiones estratégicas, clasificación y clustering de los riesgos según los factores asociados, capacitación en gestión del riesgo a directores y responsables del riesgo, se organiza la información, facilitando su análisis y presentación, apoyando las decisiones según su relevancia para el negocio.
RE2.1 Definir Alcance del Análisis de Riesgo	Capacitando a los responsables de gestión del riesgo y gestión del negocio, en la evaluación de riesgos y generando su involucramiento y compromiso con el análisis de riesgos. Por medio del acceso a la CMS, donde el CEO, CIO, CFO y responsables de la Gestión del riesgo puedan, incorporar, acceder, desarrollar, transferir y alinear el análisis del riesgo y alinearlo en conjunto con los objetivos del negocio de la organización, permite el análisis y ponderación del alcance del análisis del riesgo a nivel organizacional.	Aplicando técnicas como benchmarking, mapa de riesgos y factores de riesgo, los responsables de riesgo y negocios analizan los riesgos según la relevancia asignada, factores asociados y frecuencia a través de charlas con expertos y capacitación en análisis de riesgo. De esta forma se posibilita un análisis del riesgo a nivel organizacional, así como el compromiso con la gestión del riesgo por parte de los responsables y directores.

<p>RE2.2 Estimación de riesgos en TI</p>	<p>Capacitando a los responsables del riesgo, CRO y responsables de gestión del negocio en la determinación de los controles de riesgo con una visión global y unificada, basada en la tolerancia al riesgo definida, logrando el acuerdo y compromiso de las partes involucradas, aumentando su conocimiento y logrando así mejores resultados. Almacenando y actualizando la CMS, generando la retroalimentación para la toma de decisiones futuras, alcanzando así mejores resultados.</p>	<p>Aplicando un plan de formación y capacitación que instruya en el análisis de la información disponible (riesgos, factores de riesgo, frecuencia y magnitud de riesgo, tolerancia de riesgo, etc.), permitiendo el análisis de distintos escenarios y tipos de amenazas. Aplicando técnicas de gestión del conocimiento como ser mejores técnicas y lecciones aprendidas, así como consultas a expertos, lo cual permitirá aprovechar el conocimiento disponible del CMS, optimizando el tiempo, costo y facilitando la toma de decisiones de todas las partes involucradas.</p>
<p>RE2.3 Identificar las opciones de respuesta de riesgo</p>	<p>Junto a los directivos y responsables de gestión del riesgo y del negocio, aplicando técnicas y herramientas de gestión del conocimiento se identifican y registran los datos de respuestas de riesgo, haciendo accesible esta información para la mejor gestión de los riesgos, así como su uso en los distintos programas y proyectos de la organización.</p>	<p>Relevando la información sobre las posibles respuestas de riesgo, aplicando técnicas de gestión del conocimiento como ser capacitación en análisis de riesgos, asesoramiento con expertos, charlas formales e informales y lecciones aprendidas, generando conocimiento que será retenido en el CMS y disponible para su uso en los distintos programas y proyectos de la empresa, brindando una visión global de los mismos a nivel de la organización.</p>

<p>RE2.4 Realizar una revisión por pares de los resultados de análisis de riesgos de TI</p>	<p>Capacitando a los responsables de la gestión de riesgo en la utilización de herramientas y técnicas de gestión del conocimiento para identificar, adquirir y almacenar información sobre los recursos, sus limitaciones, requerimientos, así como en la aplicación de técnicas de análisis de la información sobre el conocimiento disponible en el CMS para facilitar y mejorar la asignación de recursos.</p>	<p>Aplicando benchmarking para obtener conocimiento externo a la organización, así como coaching, charlas con expertos y charlas informales, comunidades de prácticas, facilitando la internalización, combinación socialización y externalización del conocimiento de forma que se integra, actualiza y retiene en la base de conocimiento información sobre recursos. Aplicando sistemas expertos para la resolución de la asignación de recursos y haciendo uso del conocimiento disponible. Motivando las buenas prácticas en gestión de recursos, mejorando los tiempos y costos para la organización.</p>
<p>RE3: Mantener el perfil de riesgos</p>	<p>Por medio de la capacitación a los directivos de TI y responsables de negocio en la implementación de técnicas y herramientas de gestión del conocimiento, para la adquisición de nuevo conocimiento, desarrollo del existente y la correcta distribución y uso del mismo en la organización, optimizando el mantenimiento del conocimiento referente a riesgos, recursos y conocimiento asociado, así como la definición de indicadores que satisfagan los requerimientos de información para la gestión del plan de riesgos. Manteniendo una cultura organizacional</p>	<p>Aplicando técnicas y herramientas de gestión del conocimiento como por ejemplo mentoring, coaching, charlas informales, grupos de expertos, así como por la definición de planes de formación y capacitación específicos, mediante el uso de mapas de conocimiento y sistemas expertos que faciliten y optimicen el uso de la información disponible sobre riesgos, recursos e información relacionada.</p>
<p>RE3.1 Mapa de recursos de TI para procesos de negocio</p>	<p>Ofreciendo a los responsables de negocio y de gestión del riesgo, la aplicación de técnicas y herramientas que facilitan y organizan el conocimiento, permitiendo un mejor acceso al mismo.</p>	<p>Mediante el uso de mapas de conocimiento que facilitan la comprensión de las relaciones entre riesgos y actividades del negocio, facilitando la accesibilidad al conocimiento del CMS.</p>

<p>RE3.2 Determinar la criticidad de negocios de los recursos de TI</p>	<p>Utilizando herramientas y técnicas de gestión del conocimiento por parte de las distintas áreas involucradas en la gestión de los recursos, se capacita y facilita el uso del conocimiento para la toma de decisiones en cuanto a la criticidad de los recursos en TI, alineando la misma con los requerimientos del negocio.</p>	<p>Con el uso de técnicas de gestión del conocimiento como ser capacitación interna y externa, contacto personal con los responsables de las distintas áreas involucradas y formación de grupos de expertos, que brinden su experiencia y conocimiento en la determinación de la criticidad de recursos, haciendo uso de mapas de conocimiento y el CMS (repositorio de conocimiento), se forma a los recursos humanos en esta tarea, reduciendo los tiempos y costos de la actividad, así como obteniendo un resultado alineado con los requerimientos del negocio.</p>
<p>RE3.3 Entender las capacidades de TI</p>	<p>Con el compromiso de los responsables de TI y responsables de cada área, aplicando técnicas y herramientas de gestión del conocimiento se evalúan las capacidades disponibles y posibles ajustes a realizar, aumentando el compromiso y conocimiento de los involucrados generando mejores resultados, que contemplan la realidad de la organización y su situación actual y futura.</p>	<p>Aplicando un plan de capacitación en gestión a los responsables involucrados, obteniendo su compromiso, por medio de charlas informales, consultas a expertos y haciendo uso de mapas de conocimiento y el CMS disponible, logrando el desarrollo de nuevo conocimiento y generando la transferencia del mismo a los involucrados, obteniendo así mejores resultados para la organización.</p>

<p>RE3.4 Actualización de los componentes del escenario de riesgos de TI</p>	<p>Revisando y analizando la situación actual y futura de los componentes de los distintos escenarios de riesgo, aplicando técnicas que faciliten el desarrollo de esta actividad, capacitando a los responsables de negocios, TI y del riesgo, generando su compromiso y participación con visión a nivel de la organización.</p>	<p>Capacitando a los responsables de TI, negocio y riesgo, facilitando el análisis de los componentes y distintos escenarios, por medio de charlas con expertos, charlas informales, benchmarking, haciendo uso de mapas de conocimiento y la información del CMS, desarrollando nuevo conocimiento, habilidades e ideas, adquiriendo estas y mejorando así las decisiones futuras en base al nuevo conocimiento generado.</p>
<p>RE3.5 Mantener los riesgos de TI y mapa de registro de riesgos de TI</p>	<p>Con el uso de herramientas y técnicas de gestión del conocimiento que faciliten la construcción del perfil de riesgo, así como la actualización del conocimiento asociado a los riesgos en TI, adquiriendo y desarrollando dicho conocimiento de forma coordinada entre los responsables de TI y de negocios, alcanzando así mejores resultados para la gestión del riesgo de la organización.</p>	<p>Aplicando técnicas y herramientas que permitan a los responsables de TI y de negocio capturar el perfil de riesgo de la organización, aplicando técnicas como capacitación y charlas con expertos en evaluación de riesgos, charlas informales, utilizando mapas de conocimiento, así como benchmarking para actualizar el mapa de riesgos en TI en base a información externa a la organización, aumentando así el conocimiento y mejorando los resultados del proceso de gestión de riesgos.</p>
<p>RE3.6 Diseñar y comunicar los indicadores de riesgo de TI</p>	<p>Con el compromiso e involucramiento de la dirección de la organización en el seguimiento de los indicadores. Utilizando técnicas y herramientas para la adquisición, retención, uso y distribución de los indicadores a los administradores responsables de su gestión. Capacitando a los responsables de negocio y riesgo en la determinación de los indicadores apropiados. Generando una cultura de gestión del riesgo en la organización.</p>	<p>Aplicando técnicas de gestión del conocimiento como ser la capacitación, charlas con expertos, buenas prácticas, etc., para adquirir, retener, utilizar y distribuir los indicadores de la empresa, teniendo en cuenta las condiciones internas y externas, así como el conocimiento ya existente. Logrando el compromiso e involucramiento de la dirección, así como formando una cultura de gestión de riesgo en la organización.</p>

RE1.1 Establecer y mantener un modelo para la recolección de datos	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir y Retención, en capacitación y formación del personal, registro del conocimiento en la KDBMS por el personal adecuado.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional Patentes Análisis de redes sociales	Realidad virtual. Sistemas expertos. Charlas informales. Bases de conocimiento Elearning. Clasificación. Clustering Contacto Personal Mentoring Coaching	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RE1.2 Recopilar datos sobre el entorno externo	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	<p>Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir y Retención, intercambiando experiencias y recopilando información histórica que nutre la KDBMS de la empresa y del entorno.</p>	<p>Comunidades de práctica y grupos expertos.</p> <p>Redes, Fusión y adquisición de conocimiento.</p> <p>Mapas</p> <p>Lecciones aprendidas.</p> <p>Mejores prácticas.</p> <p>Benchmarking</p> <p>Accesibilidad.</p> <p>Memoria organizacional</p> <p>Análisis de redes sociales</p>	<p>Charlas informales.</p> <p>Bases de conocimiento.</p> <p>Contacto Personal</p> <p>Coaching</p>	<p>Recursos económicos.</p> <p>Tiempo.</p> <p>Capacitación.</p> <p>Recursos Humanos.</p> <p>Marcos de Buenas prácticas.</p> <p>Cultura organizacional.</p> <p>CKO (En caso de existir este rol).</p> <p>Compromiso de la alta gerencia.</p>

RE1.3 Recopilar datos sobre eventos de riesgo	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir y Retención, en integración de información sobre programas, proyectos, servicios existentes, etc., en la KDBMS.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Memoria organizacional	Sistemas expertos. Charlas informales. Bases de conocimiento. Contacto Personal Mentoring Coaching	Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RE1.4 Identificar factores de riesgo	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir y Retención, recopilando información sobre el vínculo entre factores de riesgo asociados con factores de riesgo ya existentes o similares.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento. Clasificación. Clustering Contacto Personal Mentoring Coaching	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RE2.1 Definir Alcance del Análisis de Riesgo	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir y Retención, en el análisis de riesgo según su relevancia, factores asociados y frecuencia.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Memoria organizacional Diseño del área de Trabajo	Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RE2.2 Estimación de riesgos en TI	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir y Retención, en capacitación sobre determinación de escenarios y tipos de amenazas.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RE2.3 Identificar las opciones de respuesta de riesgo	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir y Retención, en capacitación sobre análisis y respuestas de riesgos.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RE2.4 Realizar una revisión por pares de los resultados de análisis de riesgos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir y Retención, en el análisis y gestión sobre recursos y sus limitaciones y requerimientos.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional	Sistemas expertos. Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol).

RE3.1 Mapa de recursos de TI para procesos de negocio	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, del conocimiento sobre riesgos y actividades de negocio relacionadas.	Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional	Charlas informales. Bases de conocimiento.	Tiempo. Capacitación. Recursos Humanos. Cultura organizacional. CKO (En caso de existir este rol).

RE3.2 Determinar la criticidad de negocios de los recursos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y uso del conocimiento sobre recursos en TI.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional	Sistemas expertos. Charlas informales. Bases de conocimiento. Elearning.	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol).

RE3.3 Entender las capacidades de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación para la evaluación de capacidades en TI.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional	Charlas informales. Bases de conocimiento. Elearning. Contacto Personal	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. CKO (En caso de existir este rol).

RE3.4 Actualización de los componentes del escenario de riesgos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación para análisis de escenarios de riesgo.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional	Charlas informales. Bases de conocimiento. Elearning.	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RE3.5 Mantener los riesgos de TI y mapa de registro de riesgos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	<p>Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en construcción del perfil de riesgo y actualización del conocimiento asociado.</p>	<p>Comunidades de práctica y grupos expertos.</p> <p>Redes, Fusión y adquisición de conocimiento.</p> <p>Mapas</p> <p>Lecciones aprendidas.</p> <p>Mejores prácticas.</p> <p>Benchmarking</p> <p>Accesibilidad.</p> <p>Memoria organizacional</p> <p>Análisis de redes sociales</p>	<p>Charlas informales.</p> <p>Bases de conocimiento.</p> <p>Contacto Personal</p> <p>Mentoring</p> <p>Coaching</p>	<p>Tiempo.</p> <p>Capacitación.</p> <p>Recursos Humanos.</p> <p>Marcos de Buenas prácticas.</p> <p>Cultura organizacional.</p> <p>CKO (En caso de existir este rol).</p>

RE3.6 Diseñar y comunicar los indicadores de riesgo de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	<p>Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en construcción del perfil de riesgo y actualización del conocimiento asociado.</p>	<p>Comunidades de práctica y grupos expertos.</p> <p>Redes, Fusión y adquisición de conocimiento.</p> <p>Mapas</p> <p>Lecciones aprendidas.</p> <p>Mejores prácticas.</p> <p>Benchmarking</p> <p>Accesibilidad.</p> <p>Memoria organizacional</p>	<p>Charlas informales.</p> <p>Bases de conocimiento.</p> <p>Contacto Personal</p> <p>Mentoring</p> <p>Coaching</p>	<p>Tiempo.</p> <p>Capacitación.</p> <p>Recursos Humanos.</p> <p>Marcos de Buenas prácticas.</p> <p>Cultura organizacional.</p> <p>CKO (En caso de existir este rol).</p>

Cuadros RACI

RE1 – Recopilar datos

Funciones	Actividades principales											
	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
RE1.1 Establecer y mantener un modelo para la recolección de datos	C	C	A	R	C	C	C	C	C	I		C
RE1.2 Recopilar datos sobre el entorno externo		I	A	R	C	C	I	C	C	I	I	C
RE1.3 Recopilar datos sobre eventos de riesgo		I	A	R	R	C	C	C	C	C		I
RE1.4 Identificar factores de riesgo		C	A	R	R	I	I	C	C	R	C	C

Nota : R – Responsable A – Responsable (autoriza) C – Consultado I - Informado

RE2 – Análisis de riesgos

Funciones	Actividades principales											
	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
RE2.1 Definir alcance del análisis de riesgo	I	C	A	C	C	C	C	C	C	I	C	I
RE2.2 Estimación de riesgos en TI		I	R	C	A	I	I	C	C	I		I
RE2.3 Identificar las opciones de respuesta de riesgo			A	C	R	C	C	C	C	I		I
RE2.4 Realizar una revisión por pares de los resultados de análisis de riesgos de TI		I	A	C	C	C	I	C	C			

Nota : R – Responsable A – Responsable (autoriza) C – Consultado I - Informado

RE3 – Mantener el perfil de riesgos

Funciones Actividades principales	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
	RE3.1 Mapa de recursos de TI para procesos de negocio	I	I	A	R	R	I	I	C	C	C	I
RE3.2 Determinar la criticidad de negocios de los recursos de TI		C	A	R	R		C	C	C			
RE3.3 Entender las capacidades de TI			C	R	A		C	C	C	I	I	I
RE3.4 Actualización de los componentes del escenario de riesgos de TI		C	A	C	R	I		C	C			I
RE3.5 Mantener los riesgos de TI y mapa de registro de riesgos de TI	I	I	A	C	R	I	I	C	C	C	I	I

Nota : R – Responsable A – Responsable (autoriza) C – Consultado I - Informado

Dominio: Proceso Respuesta del Riesgo (RR)

Gestión del Riesgo Proceso Respuesta del Riesgo (RR)	Gestión del Conocimiento aplicado al Proceso Respuesta del Riesgo (RR)	Implementación de la Gestión del Conocimiento aplicado al Proceso Respuesta del Riesgo (RR)
RR1 Articular Riesgos	Aplicando técnicas y herramientas de gestión del conocimiento que logren mejorar la comunicación facilitando el acceso a las personas indicadas en el momento oportuno.	Por medio de técnicas de gestión del conocimiento que capaciten al personal en métodos y herramientas de comunicación efectivas y apropiadas para el entorno de la organización, como grupos de expertos en temas vinculados con comunicación. Utilizando mapas de conocimiento, así como la información del CMS que facilite la distribución e intercambio del conocimiento en la organización.
RR1.1 Informe de los resultados de análisis de riesgos de TI	Manteniendo informados a los directivos, responsables de negocio y de riesgo, aplicando técnicas y herramientas para una comunicación, coordinación y gestión apropiada. Adquiriendo por medio de herramientas de gestión del conocimiento los impactos positivos y negativos y comunicando los distintos escenarios que se presentan a los directivos de la organización, logrando alcanzar mejores resultados en cuanto al informe de análisis de riesgos.	Capacitando en gestión y comunicación, con charlas, mentoring, coaching, entre otras técnicas y herramientas, se logra una mejor comunicación del conocimiento, como ser pérdidas, ganancias, niveles de confianza, riesgo, etc., manteniendo informados a los responsables de negocio, directivos, etc. Aplicando técnicas como charlas, benchmarking, grupos de expertos, etc., se adquiere el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, así como su distribución y uso por medio del CMS definido a nivel de la organización.

<p>RR1.2 Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento</p>	<p>Adquiriendo, desarrollando y reteniendo el conocimiento sobre las necesidades, funciones de control y gestión de las partes interesadas, por medio de técnicas y herramientas de gestión del conocimiento. Capacitando en la generación de informes y por medio de herramientas de gestión de conocimiento logrando la distribución de información estratégica, brindando accesibilidad a todos los actores involucrados, fomentando el compromiso y generando una cultura en gestión del riesgo en la organización.</p>	<p>Haciendo uso de las herramientas y técnicas de gestión del conocimiento como ser capacitación (en la generación de informes), charlas informales, grupos de expertos, mentoring, etc., se logra adquirir, desarrollar y retener el conocimiento requerido por las partes interesadas. Con el uso de mapas de conocimiento, lecciones aprendidas y haciendo uso del conocimiento del repositorio de riesgos (CMS), se distribuye el conocimiento disponible. Generando el compromiso de toda la organización en la gestión del riesgo.</p>
<p>RR1.3 Interpretar resultados de la evaluación independiente de TI</p>	<p>Por medio del uso de un repositorio CMS de la organización, formando y capacitando al personal de gestión del riesgo y TI para el análisis del conocimiento y formación de planes de acción correctiva. Por medio de técnicas y herramientas de gestión del conocimiento se identifican oportunidades de integración con otras actividades de riesgo generando planes correctivos y difundiendo los mismos, mejorando el control de los riesgos y alineando los mismos según la gestión de riesgos de la organización.</p>	<p>Formando a los recursos humanos en el análisis del conocimiento existente en el CMS y su análisis para generar planes de acciones correctivas, así como en la identificación de oportunidades de integración con otras actividades de riesgo por medio de técnicas y herramientas como ser charlas, contacto personal, mentoring, lecciones aprendidas y mejores prácticas, difundiendo este conocimiento al resto de los involucrados.</p>

RR1.4 Identificar TI – Oportunidades relacionadas	Con la capacitación de los recursos humanos responsables de TI y de negocio en la determinación de mejores alternativas en el uso de las TI, se optimizan los recursos económicos, humanos y tiempo de la organización.	Aplicando técnicas y herramientas de gestión del conocimiento que permitan capacitar a los responsables en TI y de negocio, como ser buenas prácticas, lecciones aprendidas, capacitación en gestión de recursos, benchmarking, charlas, grupos de expertos, coaching, etc., se logra optimizar la asignación del riesgo, desarrollando y adquiriendo nuevo conocimiento para la organización.
RR2 Gestión de los riesgos de TI	Por medio de una base de conocimiento para la gestión del riesgo a nivel de la organización, aplicando técnicas de gestión del conocimiento, se logra una gestión coordinada del riesgo a nivel organizacional.	Contando con la CMS de gestión de riesgos de la organización, aplicando técnicas y herramientas como charlas, grupos de expertos, aplicando lecciones aprendidas y buenas prácticas, se gestiona en forma coordinada en base a los lineamientos estratégicos del negocio la gestión del riesgo, aprovechando las oportunidades y reduciendo el riesgo.
RR2.1 Controles del inventario	Con el uso del conocimiento del CMS y aplicando técnicas y herramientas que faciliten el acceso a la información y su interpretación, desarrollando habilidades en el control de inventario de riesgos, clasificación de controles, se adquiere conocimiento, logrando mejores resultados en la gestión de los mismos.	Haciendo uso del repositorio de conocimiento sobre riesgos, tolerancia, etc., aplicando técnicas y herramientas como ser clasificación y clustering, charlas, coaching y utilizando mapas de conocimiento, se desarrolla, adquiere y aumenta el conocimiento sobre control del riesgo, logrando mejores resultados en la gestión del mismo.

<p>RR2.2 Supervisar la alineación operacional de los umbrales de tolerancia al riesgo</p>	<p>Logrando el compromiso de la dirección, utilizando el conocimiento del CMS, se comparte y distribuye a cada área de la organización aplicando técnicas y herramientas de gestión del conocimiento que faciliten la aceptación de la rendición de cuentas, niveles de tolerancia e instrumentos de supervisión de los procesos operativos.</p>	<p>A través del acceso al conocimiento disponible en el CMS así como la capacitación y formación a la dirección. Aplicando técnicas y herramientas como grupos de expertos, charlas, lecciones aprendidas, buenas prácticas, capacitación, logrando la aceptación de las áreas operativas y dirección sobre los indicadores definidos.</p>
<p>RR2.3 Responder a la exposición al riesgo descubierto y la oportunidad</p>	<p>Facilitando el acceso al conocimiento y logrando la distribución apropiada de los cambios ocurridos aplicando técnicas de gestión del conocimiento, logrando una cultura y compromiso con la gestión del riesgo, en todas las áreas de negocio y dirección de la organización.</p>	<p>Por medio de técnicas y herramientas como mentoring, coaching, charlas y con el uso de mapas de conocimiento se logra el acceso y distribución del mismo entre los responsables y directivos de la organización, aumentando el compromiso con la gestión del riesgo y la cultura en gestión del riesgo dentro de la organización.</p>

<p>RR2.4 Implementar los controles</p>	<p>Utilizando, desarrollando y reteniendo el conocimiento sobre controles (nuevos controles o ajustes a los ya existentes), capacitando al personal en la definición, elaboración y prueba de los controles a implementar, así como identificando y adquiriendo el conocimiento sobre el personal a capacitar, se podrán lograr mejores resultados en el análisis y desarrollo de los cambios, redundando en mejoras económicas, de tiempo y en recursos humanos mejor capacitados.</p>	<p>Aplicando técnicas de gestión del conocimiento como ser coaching, mentoring, charlas, así como capacitación en la implementación de controles y uso de mapas de conocimiento se define, elabora y prueba los controles a implementar y personal a capacitar, permitiendo un mejor resultado en este proceso.</p>
<p>RR2.5 Informe del progreso del plan de acción de riesgos de TI</p>	<p>Capacitando a los responsables en TI y control del riesgo para la supervisión del plan de acción, utilizando el conocimiento del CMS de la organización, así como utilizando técnicas y herramientas que aseguren la correcta comunicación con la dirección. A través del acceso, uso, distribución y retención de los riesgos de TI de los diferentes directores de área y CEO en una base de conocimiento común (KDBMS), se podrá alinear estos a la estrategia organizacional e informar a los responsables sobre el avance y actualización necesaria del plan de acción de riesgos de TI.</p>	<p>Aplicando técnicas y herramientas de gestión del conocimiento como ser capacitación, charlas, grupos de expertos, benchmarking y haciendo uso de mapas de conocimiento de la organización, se podrá lograr alcanzar mejores resultados en la gestión de riesgos de TI, a través de una adecuada supervisión del plan de acción de riesgos de TI por medio de la comunicación y participación de la dirección, capacitación y generación de una cultura de riesgo de los recursos humanos en los procesos y actividades involucradas en el plan de acción de riesgos de TI.</p>

<p>RR3 Reacción a los acontecimientos</p>	<p>Gestionando el conocimiento a través de una base de conocimiento común (KDBMS) en la que el CEO, CIO, CFO, responsables del riesgo y directores de cada área puedan identificar, adquirir, compartir, distribuir, usar y retener el conocimiento para poder tomar decisiones en conjunto lo que permitirá reaccionar de una mejor manera los acontecimientos.</p> <p>Aplicando técnicas y herramientas de gestión del conocimiento capacitamos a los responsables de TI y de riesgo, utilizando el conocimiento del CMS de la organización.</p>	<p>Capacitando a los responsables de TI y riesgo, aplicando técnicas y herramientas como benchmarking, grupos expertos, charlas y mentoring, utilizando el conocimiento del CMS, estableciendo el compromiso y apoyo de la gerencia y asegurando el uso oportuno y eficaz de las medidas a aplicar ante la reacción a un acontecimiento.</p>
<p>RR3.1 Mantener los planes de respuesta a incidentes</p>	<p>Utilizando el repositorio de conocimiento (CMS) y por medio de técnicas y herramientas de gestión del conocimiento, se podrá identificar, Adquirir, Desarrollar, Compartir, distribuir y usar los planes de respuesta a incidentes y sus cambios a los involucrados, reteniendo así el conocimiento existente y transfiriendo el mismo a otros involucrados, mejorando de esta manera la comunicación y desarrollo de los planes de acción a incidentes en todas las áreas de la organización.</p>	<p>Capacitando a los responsables de TI y de riesgo en técnicas y herramientas como benchmarking, charlas, grupos de expertos en temas de comunicación, gestión y desarrollo de planes de respuesta, se podrá lograr la internalización, externalización, socialización y combinación del conocimiento entre las distintas áreas de la organización, mejorando la comunicación y sinergias dentro de la empresa lo que permitirá un eficiente mantenimiento de los planes de respuesta a incidentes.</p>

<p>RR3.2 Supervisión de riesgos de TI</p>	<p>Capacitando a los responsables del riesgo y auditores, gestionando la situación según el conocimiento del CMS sobre riesgos y límites que han superado la tolerancia al riesgo. Mejorando la transferencia en el conocimiento sobre el impacto a los responsables en la toma de decisiones de la organización y generando de esta manera un mayor compromiso en el seguimiento de las acciones para mejorar la gestión de riesgos desde la gestión del conocimiento.</p>	<p>Haciendo uso del conocimiento del repositorio de la organización (CMS), aplicando técnicas y herramientas como grupos de expertos, charlas y mapas de conocimiento, que posibiliten una mejora en la auditoría de los riesgos de TI, el conocimiento de los niveles y límites de riesgo tolerados y la comunicación a los responsables de cada área, facilitando el conocimiento con la correcta distribución del mismo, generando un mayor compromiso con el seguimiento de las acciones en base al riesgo y límites definidos.</p>
<p>RR3.3 Iniciar planes de respuesta a incidentes</p>	<p>Aplicando técnicas y herramientas de gestión del conocimiento se podrán identificar las categorías de hechos y su vínculo con las posibles respuestas del plan de respuestas, así como la correcta comunicación de las medidas tomadas. A través de la definición y utilización de una base de conocimiento (KDBMS) en la organización, se podrán lograr los mejores resultados para tomar la acción correcta en la resolución de los incidentes.</p>	<p>Por medio de la capacitación y formación a los responsables de la gestión y el riesgo en la organización y utilizando técnicas y herramientas como benchmarking y charlas, se podrán lograr las mejores respuestas a incidentes, y a través de la utilización de la base de conocimiento de la organización, se podrá distribuir el conocimiento a las partes interesadas en el incidente a tratar, asegurando de esta manera que se está tomando la acción correcta como respuesta a un incidente.</p>

<p>RR3.4 Comunicar las lecciones aprendidas de eventos de riesgo</p>	<p>Con la capacitación de los responsables en TI y riesgo, en la identificación, adquisición, desarrollo, análisis, compartir o distribuir, uso y retención del conocimiento de la CMS en cuanto a datos históricos y hechos recientes de acontecimientos adversos y pérdidas, aplicando técnicas y herramientas que permitan la identificación de las causas posibles de los problemas, así como la comunicación sobre requisitos adicionales de respuesta y mejoras en los procesos. Logrando de esta forma con el apoyo y capacitación de la gerencia, un marco de buenas prácticas y cultura organizacional de compromiso con la gestión del riesgo, a través del desarrollo de la gestión del conocimiento en la organización.</p>	<p>Capacitando a los responsables en TI y en riesgos para la identificación, adquisición, desarrollo, análisis, compartir o distribuir, uso y retención del conocimiento sobre datos históricos y eventos recientes, aplicando técnicas como lecciones aprendidas, benchmarking, charlas, grupos de expertos, que faciliten la identificación de las causas de problemas, desarrollando y reteniendo así el nuevo conocimiento en el CMS de la organización, así como gestión de la comunicación al resto de la organización sobre las lecciones aprendidas en el análisis realizado. Capacitando a la gerencia de manera de lograr implementar una cultura de gestión del conocimiento que apoye a la gestión del riesgo en la organización.</p>
--	---	---

RR1.1 Informe de los resultados de análisis de riesgos de TI	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación sobre comunicación y distribución del conocimiento sobre riesgo, pérdidas, ganancias y confianza.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RR1.2 Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, capacitando en la generación de informes, distribución de información estratégica y accesibilidad al conocimiento sobre la gestión de riesgo y estado de cumplimiento.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RR1.3 Interpretar resultados de la evaluación independiente de TI	Etapas implicadas (Fases)	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación y análisis de conocimiento para la formación de planes de acción correctiva.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol).

RR1.4 Identificar TI – Oportunidades relacionadas	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación sobre las mejores alternativas en el uso de las TI.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional	Sistemas expertos. Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol).

RR2.1 Controles de inventario	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en el desarrollo de habilidades en el control y gestión de inventarios de riesgo.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional	Charlas informales. Bases de conocimiento. Elearning. Clasificación. Clustering Contacto Personal Mentoring Coaching	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol).

RR2.2 Supervisar la alineación operacional de los umbrales de tolerancia al riesgo	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación sobre técnicas y herramientas para el logro de la aceptación de la rendición de cuentas, niveles de tolerancia y procesos operativos de supervisión.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RR2.3 Responder a la exposición al riesgo descubierto y la oportunidad	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en la formación en la respuesta a los cambios ocurridos sobre riesgos y oportunidades.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento.	Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RR2.4 Implementar los controles	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación para la definición, elaboración y prueba de controles.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol).

RR2.5 Informe del progreso del plan de acción de riesgos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación en supervisión y comunicación del progreso en planes de acción de riesgos.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional Análisis de redes sociales	Sistemas expertos. Charlas informales. Bases de conocimiento. Elearning.	Recursos económicos. Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RR3.1 Mantener los planes de respuesta a incidentes	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación en comunicación, gestión y desarrollo de planes de respuesta.	Comunidades de práctica y grupos expertos. Redes, Fusión y adquisición de conocimiento. Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional	Charlas informales. Bases de conocimiento. Elearning.	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol).

RR3.2 Supervisión de riesgos de TI	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación en la supervisión de riesgos y límites.	Comunidades de práctica y grupos expertos. Mapas Lecciones aprendidas. Mejores prácticas. Accesibilidad. Memoria organizacional Diseño del área de Trabajo Análisis de redes sociales	Sistemas expertos. Charlas informales. Bases de conocimiento. Elearning. Contacto Personal Mentoring Coaching	Tiempo. Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol). Compromiso de la alta gerencia.

RR3.3 Iniciar planes de respuesta a incidentes	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación en comunicación e identificación de categorías de hechos y vínculo con posibles respuestas.	Mapas Lecciones aprendidas. Mejores prácticas. Benchmarking Accesibilidad. Memoria organizacional Análisis de redes sociales	Charlas informales. Bases de conocimiento. Elearning. Clasificación. Clustering Contacto Personal Mentoring Coaching	Capacitación. Recursos Humanos. Marcos de Buenas prácticas. Cultura organizacional. CKO (En caso de existir este rol).

RR3.4 Comunicar las lecciones aprendidas de eventos de riesgo	Etapas (Fases) implicadas	Herramientas	Técnicas	Factores Implicados
	<p>Identificación, Generación, Codificación, Transferencia, Compartir o Distribuir, Retención y Uso, en capacitación en cuanto al análisis de datos históricos y recientes, así como la comunicación sobre respuestas y mejoras en los procesos.</p>	<p>Comunidades de práctica y grupos expertos.</p> <p>Mapas</p> <p>Lecciones aprendidas.</p> <p>Mejores prácticas.</p> <p>Benchmarking</p> <p>Accesibilidad.</p> <p>Memoria organizacional</p> <p>Análisis de redes sociales</p>	<p>Charlas informales.</p> <p>Bases de conocimiento.</p> <p>Elearning.</p>	<p>Capacitación.</p> <p>Recursos Humanos.</p> <p>Marcos de Buenas prácticas.</p> <p>Cultura organizacional.</p> <p>CKO (En caso de existir este rol).</p> <p>Compromiso de la alta gerencia.</p>

Cuadros RACI

RR1 – Articular riesgos

Funciones	Actividades principales											
	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
RR1.1 Informe de los resultados de análisis de riesgos de TI	I	I	R	R	C	C	A	R	R	R	C	I
RR1.2 Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	I	I	R	C	R	C	A	C	C	C	C	C
RR1.3 Interpretar resultados de la evaluación independiente de TI	I	I	A	C	R	I	I			C	I	C
RR1.4 Identificar TI – Oportunidades relacionadas		I	R	R	R	I	A	R	R	R	I	I

Nota : R – Responsable A – Responsable (autoriza) C – Consultado I – Informado

RR2 – Gestión de los riesgos de TI

Funciones	Actividades principales											
	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
RR2.1 Controles del inventario		I	A	R	C	I	I	C	C	R		C
RR2.2 Supervisar la alineación operacional de los umbrales de tolerancia al riesgo			A	C	C		I	R	R	R		C
RR2.3 Responder a la exposición al riesgo descubierto y la oportunidad	I	A	C	R	R	C	I	R	R	C	C	
RR2.4 Implementar los controles	I	A	C	C	R	C	I	R	R	C	C	I
RR2.5 Informe del progreso del plan de acción de riesgos de TI	I	I	R	R	R	I	A	R	R	R	I	I

Nota : R – Responsable A – Responsable (autoriza) C – Consultado I - Informado

RR3 – Reacción a los acontecimientos

Funciones	Actividades principales											
	Directivos	Director Ejecutivo (CEO)	Jefe de Riesgo (CRO)	Jefe de Conocimiento (CKO)	Jefe de Información (CIO)	Jefe Financiero (CFO)	Comité de Riesgos	Gestión Empresarial	Dueño de procesos de negocio	Funciones de control de Riesgo	Recursos Humanos	Auditoría y Control
RR3.1 Mantener los planes de respuesta a incidentes	I	I	R	R	R	C	A	R	R	R	C	I
RR3.2 Supervisión de riesgos de TI			A	C	C	I	I	R	R	R	C	R
RR3.3 Iniciar planes de respuesta a incidentes	I	I	A	C	C	I	C	R	R	R	C	I
RR3.4 Comunicar las lecciones aprendidas de eventos de riesgo	I	I	A	R	R	C	I	C	C	R	C	I

Nota : **R** – Responsable **A** – Responsable (autoriza) **C** – Consultado **I** – Informado

Anexo XV – Matrices del Modelo de Gestión del Riesgo basado en la Gestión del Conocimiento

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
Estrategia de TI				
Nivel 1: Básico	<p>La organización no reconoce la necesidad de administrar la exposición al riesgo del negocio y sus operaciones, o el reconocimiento está surgiendo pero se limita a evitar riesgos para cumplir con los requisitos o transferencia del riesgo a través de seguros. No existe una base de conocimiento que cuente con los objetivos organizacionales y las acciones a ejecutar por cada área para el logro de los objetivos. Solo existe una identificación ad hoc del conocimiento para cumplir con las actividades propias del negocio. En ocasiones se utilizan algunas herramientas como redes, fusión y adquisición del conocimiento. Se carece de una cultura, buenas prácticas y compromiso de la</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico y no se ve un beneficio en su consideración. Los criterios de identificación de riesgo de TI varían en toda la organización según el criterio de cada usuario / área. En ocasiones se utilizan herramientas y técnicas de gestión del conocimiento como cámaras web, videoconferencias y realidad virtual solo a nivel del cumplimiento de las tareas.</p>	<p>TI es considerado responsable de la evaluación de riesgos y las opciones de mitigación se deducen de la evaluación de los hechos ocurridos. Las habilidades de gestión de riesgos pueden existir sobre una base ad hoc, pero no son desarrolladas activamente. Ante la no existencia de una base de conocimiento organizacional, los controles se basan en requisitos de cumplimiento que pueden variar ampliamente en relación al riesgo y operar en áreas aisladas.</p>	<p>Los eventos de TI y las condiciones que pueden afectar el día a día en las operaciones en ocasiones se discuten en reuniones de gestión, pero las respuestas de riesgo específicos no se consideran. El apetito y tolerancia al riesgo solo se consideran en evaluaciones de hechos ocurridos. Los inventarios ad hoc centrados en el control se encuentran dispersos en aplicaciones de escritorio. No existe una identificación sistemática del conocimiento necesario para la operativa del negocio. Ocasionalmente se aplican herramientas como redes, fusión y adquisición del conocimiento, así como el uso de cámaras web, videoconferencias y realidad virtual. El factor tiempo y los recursos financieros inciden en la gestión del conocimiento, no existiendo una cultura organizacional de gestión del conocimiento, así como la aplicación de un marco de buenas prácticas.</p>

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	gerencia para la gestión del conocimiento en la gestión del riesgo.			
Nivel 2: Gestionada y establecida	Se considera la gestión de riesgos como una cuestión empresarial capacitando y formando a los directores en el uso del conocimiento sobre riesgo. Se designa un líder para la gestión de riesgos de TI (CRO) en toda la empresa, así como para la gestión del conocimiento (CKO). Se definen las competencias requeridas y son documentadas para todas las áreas de riesgo de la empresa. Actividades de gestión del riesgo alineadas en toda la empresa, aplicando herramientas de gestión del conocimiento como lecciones aprendidas y grupos de expertos.	Usuarios de TI capacitados en amenazas relacionadas a TI, escenarios de riesgo, mitigación y control asociados a su función y responsabilidades, con la aplicación de técnicas como cámaras web, videoconferencias, realidad virtual, externalizando el conocimiento sobre riesgo, mitigación y control por medio de comunidades de práctica y grupos de expertos.	Existe una formación y sensibilización del personal en cuanto a riesgos y se maneja un lenguaje común para la comunicación de riesgos dirigida y gestionada por el CKO. Se define un inventario centralizado de los problemas de riesgo, definiendo una base de conocimiento común a toda la organización. Por medio de herramientas como grupos de expertos y comunidades de práctica, aplicando lecciones aprendidas, fomentando la cultura organizacional en la gestión del riesgo.	Se utilizan herramientas para la gestión del riesgo en la operativa del negocio y herramientas de gestión del conocimiento que facilitan la capacitación de los recursos humanos como ser adquisición del conocimiento, fusión y redes. Existen políticas de respuesta a los riesgos que definen cuándo y cómo responder a estos. Se destina tiempo y recursos económicos en la capacitación de los RRHH, con el compromiso de la gerencia y la gestión del CKO, lo cual permite una adecuada gestión del riesgo aplicado a la operativa de la organización.
Nivel 3: Predecible	Las políticas y normas de la empresa reflejan la tolerancia al riesgo empresarial. Se	La empresa se ocupa del desarrollo a largo plazo de las necesidades	La gestión de riesgos se ve como facilitador de negocios y se entiende y	La evaluación de la eficiencia y eficacia de los riesgos son medidos y comunicados, así como relacionados con los

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	<p>planifica los escenarios de riesgo considerando los riesgos de TI en toda la empresa. Una cultura de la recompensa motiva la acción positiva. El proceso de gestión de riesgos se documenta y se gestiona cuantitativamente, así como la gestión del conocimiento que es retenido en una base de conocimiento organizacional, facilitando la internalización y combinación de éste en toda la organización. Existe un compromiso explícito de la alta gerencia y de todos los RRHH de la organización en cuanto a la gestión del conocimiento en riesgos. Se recurre a la búsqueda e identificación de marcos de buenas prácticas para este fin.</p>	<p>de personal con alto potencial en evaluación de riesgos y técnicas relacionadas. Se aplican herramientas de análisis de riesgo basadas en un plan estándar, e integradas con otras herramientas relacionadas. Los requisitos de habilidad son actualizados rutinariamente en todas las áreas, por medio de herramientas y técnicas de gestión de conocimiento como accesibilidad y diseño del área de trabajo, charlas informales, contacto personal y e-learning, favoreciendo una cultura de gestión de riesgos en toda la organización.</p>	<p>gestiona la baja y alza de riesgos en TI, donde se comparte, usa, retiene y desarrolla el conocimiento sobre riesgos, factores asociados, respuesta a riesgos, por medio de técnicas y herramientas como mapas de conocimiento, patentes, análisis de redes y memoria organizacional.</p>	<p>objetivos de negocio y plan estratégico de TI. El papel del departamento de TI en la gestión del riesgo operacional es entendido y aplicado. El conocimiento se desarrolla en todas sus fases de socialización, externalización, internalización y combinación, por medio de una base de conocimiento común, logrando la transferencia del conocimiento en toda la organización, con el uso de técnicas como, charlas informales, contacto personal y e-learning.</p>
Nivel 4: Optimizada	<p>Los altos ejecutivos consideran en sus decisiones todos</p>	<p>Los responsables de las decisiones</p>	<p>La empresa exige formalmente la mejora continua</p>	<p>TI es un actor importante en la línea de los esfuerzos empresariales de riesgo operacional. Se</p>

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	<p>los aspectos de riesgos en TI y disponen de la mejor información acerca de probabilidades de pérdida, riesgos y oportunidades. Las estrategias de respuesta de riesgo son aplicadas de manera integral, justificada y controles costo-eficacia mitigan la exposición al riesgo en forma continua. Aplicando una gestión del conocimiento definida y gestionada por el CKO y contando con el compromiso de la alta gerencia y de todos los RRHH, se favorece la mejora continua a través de la utilización de todas las técnicas y herramientas disponibles de gestión del conocimiento, contemplando la realidad del entorno y de la organización, a través de grupos expertos, comunidades de prácticas, mejores prácticas, mapas de conocimiento y benchmarking.</p>	<p>disfrutan de la transparencia en los riesgos de TI y disponen de la mejor información acerca de las probabilidades de pérdida, riesgos y oportunidades. Se desarrolla, distribuye, usa y retiene el conocimiento con el compromiso de los usuarios en la mejora continua de sus funciones, lo que permite que los procesos de gestión del riesgo orientado a éstos mejoren en forma permanente.</p>	<p>de la gestión de las capacidades de los riesgos de TI basada en objetivos claramente definidos de personal y de organización. Existe un seguimiento en tiempo real de los eventos y excepciones de control al igual que la automatización de la gestión política. Existe un compromiso de la alta gerencia y cultura organizacional que permiten gestionar la capacitación constante de los recursos humanos en la gestión del riesgo alineado al negocio. Se aplican herramientas y técnicas de gestión del conocimiento como sistemas expertos, ajustándose de la mejor manera para el logro de la mejora continua, desarrollando la base de conocimiento</p>	<p>exige formalmente la mejora continua de la recogida de datos, análisis de riesgos y perfiles de competencias. Herramientas automatizadas apoyan y mejoran la evaluación de riesgos, así como la respuesta a los mismos para inteligentemente asumir riesgos adicionales y aprovechar oportunidades optimizando los factores de tiempo y recursos económicos. Herramientas y técnicas de gestión del conocimiento facilitan estas actividades y se desarrollan en un proceso de mejora continua, tales como clasificación, clustering, e-learning, mentoring y coaching, con RRHH comprometidos y capacitados, en base a la utilización de marcos de buenas prácticas, fomentando y manteniendo la cultura de la gestión del riesgo en toda la organización.</p>

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
			organizacional.	
Portfolio estratégico	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
Nivel 1: Básico	Los proyectos que forman parte del incipiente portfolio son aquellos que permiten automatizar tareas repetitivas buscando reducir costos. No se lleva un registro de riesgos, factores de riesgo, formas de mitigarlos, soluciones aplicadas y su resultado, de forma que puedan ser utilizados por el conjunto de proyectos del portfolio y/o la organización en su conjunto. La identificación del conocimiento se limita a hechos ocurridos sobre tareas repetitivas. Se pueden aplicar algunas herramientas como redes, fusión y adquisición del conocimiento, pero no está definido un marco de buenas prácticas para la aplicación en los proyectos del portfolio, ni una cultura de gestión del conocimiento en riesgos. Los	El portfolio incluye con más énfasis los requisitos de los usuarios lo que implica una falta de visión estratégica en el mismo. No existe o es escaso el conocimiento sobre los riesgos implicados por tipo de usuario, expectativas, experiencias anteriores. Se pueden identificar riesgos, factores de riesgo y respuestas, pudiendo utilizar herramientas y técnicas de gestión del conocimiento como cámaras web, videoconferencias y realidad virtual, sin seguir un marco de buenas prácticas.	El portfolio está orientado a las operaciones más que a contribuir a la estrategia del negocio. Se esbozan planes de gestión de riesgo de los proyectos del portfolio a partir del departamento de TI, quien es responsable de la gestión de problemas, disponibilidad y acceso al sistema. Aún no existe una cultura de gestión del conocimiento que permita hacer uso de una base de conocimiento organizacional, por lo que los controles a aplicar en el portfolio de proyectos se basan en requisitos de cumplimiento que pueden variar en relación al riesgo con respecto al resto de la organización y entre proyectos	No siempre el portfolio está articulado para brindar servicios con los niveles esperados. Las habilidades de gestión del riesgo pueden existir sobre una base ad hoc pero no son desarrolladas activamente. La identificación del conocimiento no se realiza en forma sistemática, aplicando ocasionalmente herramientas como redes, fusión y adquisición del conocimiento, así como el uso de cámaras web, videoconferencias y realidad virtual. El factor tiempo, recursos humanos y recursos financieros inciden en la gestión del conocimiento, no está instaurada una cultura de gestión del conocimiento en los RRHH involucrados en el portfolio.

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	responsables de la gestión del portfolio no presentan un compromiso explícito con la gestión del conocimiento.		del mismo portfolio. Se aplican técnicas de gestión del conocimiento como redes, fusión y adquisición del conocimiento de forma no coordinada.	
Nivel 2: Gestionada y establecida	Desde que las estrategias de TI y del negocio están alineadas, el portfolio se convierte en un elemento estratégico, de forma incipiente en este nivel de madurez. Se gestionan de manera incipiente los riesgos del portfolio. Se gestiona el riesgo en base a un inventario centralizado de riesgos de la organización, con el apoyo del CKO en la gestión del conocimiento. Se definen las competencias requeridas y son documentadas para todos los proyectos del portfolio. Actividades de gestión del conocimiento facilitan la gestión del riesgo, aplicando	Existen procesos definidos que establecen la forma y las prioridades tanto de los usuarios como del negocio. El portfolio se gestiona estratégicamente. Se forman los recursos humanos involucrados y se sensibiliza en riesgos, manejando un lenguaje común para todos los proyectos, aplicando técnicas de gestión del conocimiento como comunidades de práctica, y mejores prácticas, externalizando e internalizando el conocimiento	El portfolio refleja el alineamiento entre TI y el negocio aportando valor al mismo. Están definidas y documentadas las necesidades de competencias para el portfolio de proyectos, considerando la recolección de datos, análisis de riesgos y perfiles. Se definen los responsables de respuesta ante riesgos. Se aplican técnicas de gestión del conocimiento para la identificación, adquisición y desarrollo del conocimiento sobre riesgos aplicado al portfolio, como mapas de conocimiento, patentes, comunidades de	La gestión se realiza teniendo en cuenta los niveles de servicio establecidos por los procesos. Estos han sido definidos de acuerdo con la arquitectura y la infraestructura actual y futura de TI. La tolerancia al riesgo del portfolio está alineada a TI y al negocio. Se definen los recursos económicos y humanos para el portfolio de proyectos, en coordinación con el CKO, de forma de gestionar el tiempo necesario para la capacitación de los RRHH, para la adecuada operativa, aplicando técnicas y herramientas como mapas de conocimiento, comunidades de práctica, mejores prácticas y análisis de redes sociales.

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	herramientas como lecciones aprendidas y grupos de expertos.	en todos los proyectos del portfolio de forma coordinada.	práctica, grupos de expertos, mejores prácticas y análisis de redes sociales.	
Nivel 3: Predecible	La capacidad actual y futura del portfolio se mide de acuerdo a los procesos definidos por la organización. Es bien vista la gestión de riesgos en el portfolio y los roles están claramente definidos. Se planifican prudentemente los escenarios de riesgo, considerando los riesgos en TI asociados al portfolio y alineados al plan de riesgos de la organización, reteniendo el conocimiento en una base de conocimiento organizacional, la cual es utilizada por todos los proyectos del portfolio, facilitando de esta manera la internalización, externalización, y combinación del conocimiento, mediante el uso de marcos de buenas prácticas y	Se mide cuantitativamente el proceso definido para la gestión del portfolio en función de las necesidades del usuario pero con una visión de integración estratégica con el negocio. Se analiza a largo plazo las necesidades de personal capacitado en evaluación del riesgo, aplicando técnicas y herramientas como mentoring, coaching, charlas informales y contacto personal.	Se mide el aporte de TI al negocio de acuerdo a los procesos definidos. Se desarrolla la base de conocimiento de riesgos de la organización para lograr el mejor resultado en el análisis y evaluación de riesgos y respuestas, utilizando y midiendo el uso de herramientas como comunidades de práctica, redes, mejores prácticas y análisis de redes sociales aplicados sistemáticamente. Existe un compromiso explícito de los responsables del portfolio y de TI, para la gestión de riesgos.	Se mide la eficiencia y eficacia de la gestión de riesgos en el portfolio, se comunican y son relacionados con el objetivo de la organización y de TI. Los requisitos de habilidad son rutinariamente actualizados para todas las zonas de riesgo identificadas en el portfolio de proyectos, así como los riesgos y su mitigación, reaccionando así a los acontecimientos y oportunidades que se presentan, con la aplicación de técnicas y herramientas como mentoring, coaching, grupos de expertos y charlas informales, obteniendo una capacitación ajustada a los requerimientos de cada proyecto.

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	herramientas como comunidades de práctica y grupos expertos.			
Nivel 4: Optimizada	<p>El portfolio está organizado de acuerdo a las estrategias y metas actuales y futuras. Se toman en cuenta los riesgos y las regulaciones de la organización, con una gestión del conocimiento definida para el portfolio y gestionada con el CKO, contando con el compromiso de los directores del portfolio, haciendo uso del repositorio de conocimiento KDMBS de la organización. Se mide y se mejora de forma continua la gestión de las capacidades en el riesgo basados en objetivos claramente definidos para el portfolio. Se utilizan todas las herramientas y técnicas de gestión del conocimiento que mejor se ajusten, como clasificación y clustering, e-learning, mapas de conocimiento y benchmarking. Se capacita y se</p>	<p>El portfolio se gestiona de acuerdo a las necesidades de los usuarios y en conformidad con las estrategias del negocio, su arquitectura y la infraestructura necesaria. En base a la comprensión de todos los requisitos se hace frente al riesgo, el cual se mide y se mejora continuamente, para lo cual se aplican técnicas y herramientas de gestión del conocimiento como accesibilidad y diseño del área de trabajo, según mejor se ajusten a la situación, en forma sistemática y planificada.</p>	<p>Se gestionan y priorizan los programas y proyectos de acuerdo a su valor económico, teniendo en cuenta el conjunto de intangibles que inciden en el valor real de cada proyecto del portfolio y el riesgo asociado. Se aplica de forma integral estrategias de respuesta al riesgo mitigando la exposición al mismo de forma continua, a través del uso de herramientas y técnicas de gestión del conocimiento como mentoring, coaching, contacto personal, charlas informales, mapas de conocimiento, con el compromiso de todos los recursos humanos en</p>	<p>Se toman en cuenta las habilidades necesarias para que se puedan cumplir las metas propuestas de gestión de riesgo. Un elemento eje es la capacitación de los RRHH que desarrollan el portfolio, para lo cual se aplican técnicas y herramientas de gestión del conocimiento como coaching, mentoring, charlas informales, fusión o adquisición de conocimiento, entre otros, en un proceso de mejora continua, a través de una base unificada de conocimiento de gestión del riesgo de la organización. Con el seguimiento y control de la gestión del tiempo y recursos humanos para el desarrollo de las actividades del portfolio.</p>

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	educa en el aprendizaje del conocimiento sobre tecnologías avanzadas de respuesta de riesgos, de forma de poder entender y asumir riesgos adicionales y aprovechar nuevas oportunidades.		asumir su responsabilidad frente al riesgo, gestionando la incertidumbre y aprovechando las oportunidades.	
Proyectos				
Nivel 1: Básico	Los proyectos que se implementan son aquellos que permiten bajar los costos y/o automatizar procesos repetitivos. No se define un registro de riesgos, factores de riesgo, formas de mitigarlos, soluciones aplicadas y su resultado. Se pueden aplicar algunas herramientas como redes, fusión y adquisición del conocimiento, pero no está definido un marco de buenas prácticas para su aplicación en el proyecto.	Proyectos seleccionados por presiones de los usuarios más que por su valor dentro del negocio. No existe un estudio de riesgo o no está definido claramente, que evalúe la aceptación de los usuarios, sus requisitos y necesidades, lo cual impacta en factores económicos y de tiempo. Ocasionalmente se identifican riesgos, factores y respuestas al riesgo, pudiendo utilizar herramientas y técnicas de gestión del conocimiento como cámaras web,	Los riesgos en TI y factores de respuesta al mismo, se pueden identificar sin seguir un estándar o marco de buenas prácticas. No existe un compromiso explícito de la dirección en la gestión del riesgo. El tiempo y los recursos económicos asignados al proyecto pueden no incluir los costos asociados a la mitigación del riesgo.	El proyecto no se desarrolla mediante un proceso definido, estándar y comunicado. No existe un compromiso explícito en la gestión del riesgo por parte de los responsables del proyecto, pudiendo existir socialización del conocimiento por medio de cámaras web, videoconferencias y realidad virtual, así como redes, fusión y adquisición del conocimiento. No se define una capacitación y formación de los recursos humanos para la gestión del conocimiento en riesgo.

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
		videoconferencias y realidad virtual, sin un marco de buenas prácticas.		
Nivel 2: Gestionada y establecida	Los proyectos son seleccionados de acuerdo a las prioridades del negocio y según las estrategias definidas. Las categorías de riesgo que aplican al proyecto se han identificado, se formó y sensibilizó a los recursos humanos asignados al proyecto en riesgos, se definió la comunicación de riesgos basada en una base de conocimiento organizacional, con el apoyo del CKO. Se aplican técnicas y herramientas que facilitan el intercambio de conocimiento. Se asignan los recursos económicos y humanos para una correcta gestión del riesgo. Se cuenta con el compromiso de la dirección del proyecto y se genera una cultura en riesgo entre los	Existen procesos definidos que establecen qué proyectos desarrollar teniendo en cuenta las necesidades de los usuarios y las estrategias del negocio. Se capacita y forma para mitigar el riesgo de fracaso en el proyecto teniendo en cuenta los usuarios del mismo, contemplando experiencias anteriores, utilizando técnicas y herramientas de gestión del conocimiento que permitan adquirir, desarrollar y compartir el conocimiento, como lecciones aprendidas, comunidades de práctica, grupos de	Los proyectos seleccionados deberán estar dentro del conjunto de aquellos que contribuyen a las estrategias del negocio. La gestión del riesgo del proyecto está definida, así como la adquisición y desarrollo del conocimiento sobre riesgos del proyecto en todas sus etapas.	Existen procesos definidos, comunicados y estandarizados que establecen los niveles, umbrales, perfiles y escenarios de riesgo, así como controles y responsabilidades. Se utilizan herramientas y técnicas para la gestión del conocimiento en riesgo como comunidades de práctica, redes, mejores prácticas y análisis de redes sociales.

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	integrantes del proyecto alineada con la gestión de riesgos de la organización.	expertos, mejores prácticas y análisis de redes sociales.		
Nivel 3: Predecible	Se gestiona el riesgo según el plan de gestión del riesgo de la organización y es entendido como un facilitador para el proyecto. Está definido el apetito al riesgo y la tolerancia al riesgo para el proyecto. Se planifica los escenarios de riesgo considerando los riesgos de TI aplicado al proyecto. Se cuenta con un plan de formación y capacitación en riesgos y se aplican herramientas y técnicas como accesibilidad y diseño del área de trabajo, mapas de conocimiento y patentes, que facilitan los procesos de externalización, interiorización, combinación y socialización del conocimiento en riesgos para el proyecto.	Se cuenta con un plan de formación y capacitación periódica en amenazas, escenarios de riesgo, controles y responsabilidades, respondiendo a los riesgos que se presenten en cuanto a la relación con los usuarios, identificando las deficiencias en el control y remediándolas de forma oportuna. Se asignan los recursos humanos y tiempo para esta capacitación, la cual se realiza aplicando técnicas y herramientas de gestión del conocimiento como coaching, mentoring, charlas informales y contacto personal.	La eficiencia y eficacia de los riesgos se miden, comunican y se relacionan con los objetivos de negocio y el plan estratégico de TI. La dirección comprometida con la gestión de riesgos, en conjunto con TI determina si una condición de riesgo es superior a la tolerancia definida. Existe una comprensión del impacto de las amenazas de negocio así como las acciones a tomar en caso de que ocurran. Todos los aspectos del proceso de respuesta a los riesgos se documentan y son cuantitativamente gestionados en el proyecto. Se utilizan las herramientas y técnicas de	El papel de TI en la gestión del riesgo operacional y de negocio está definido claramente. Los requisitos de habilidad son rutinariamente actualizados para todas las zonas de riesgo identificadas en el proyecto, así como los riesgos y su mitigación, con la aplicación sistemática de técnicas y herramientas como mentoring, coaching, sistemas expertos, e-learning, haciendo uso de la base de conocimiento organizacional.

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
			gestión del conocimiento como ser clasificación y clustering, coaching, mentoring, charlas informales y contacto con el personal, para la formación en supervisión de los controles críticos, capacidades y recursos.	
Nivel 4: Optimizada	Los proyectos desarrollados seleccionados del conjunto de proyectos que conforman el portfolio consideran los aspectos de riesgos en TI. El responsable de la gestión del riesgo es asesor de confianza y se dispone de la mejor información sobre riesgos y oportunidades. Aplicando marcos de buenas prácticas a través de una cultura de gestión del conocimiento, los recursos humanos del proyecto utilizan estrategias de respuesta de riesgo del proyecto que están en línea con las estrategias	El objetivo es maximizar la percepción de valor que tiene el usuario de los servicios que brinda TI, así como la comprensión de todos los requisitos para hacer frente al riesgo, que es mejorada por la transparencia en la gestión de riesgos y disponer de la mejor información posible acerca de las probabilidades de pérdida, riesgos y oportunidades, obtenida por un proceso de generación, codificación y	Se deben incluir los elementos de calidad habituales del desarrollo de proyectos y gestión de riesgos, a través de un proceso de mejora continua en la aplicación de la gestión del conocimiento, utilizando las mejores técnicas y herramientas como mapas de conocimiento y sistemas expertos.	Los proyectos son desarrollados con el objetivo de brindar los niveles de calidad de servicio esperados, el conocimiento sobre riesgos, factores de riesgo, respuesta a riesgos, son comunicados activamente a todos los involucrados en el proyecto, por medio del uso de herramientas y técnicas de gestión del conocimiento como clasificación y clustering, e-learning, haciendo uso de las bases de conocimiento organizacional de una forma sistemática y a través de un proceso de mejora continua que brinde los mejores resultados en la operativa del proyecto.

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	de la organización y son aplicadas de manera integral, justificada y controles costo-eficacia responden a la exposición al riesgo en forma continua para su control y gestión.	transferencia del conocimiento apropiado y ajustado al proyecto, con la aplicación de las herramientas y técnicas de gestión del conocimiento que mejor se ajustan como ser charlas informales, contacto personal, coaching y mentoring.		
Operaciones				
Nivel 1: Básico	Las operaciones se controlan de forma individual. No hay una clara visión a futuro de los servicios, por lo cual la información sobre riesgos y su mitigación se deducen de lo ocurrido en el momento. Las habilidades de gestión pueden existir pero no son desarrolladas activamente. Los controles sobre riesgos se basan en requisitos de cumplimiento y varían ampliamente según el riesgo. El conocimiento es generado en forma	Es importante la calidad de servicio en las operaciones, no hay estándares definidos. La identificación de los riesgos varía ampliamente en toda la organización y en TI, así como los recursos humanos reconocen o son conscientes del concepto de gestión del conocimiento en riesgos, pudiendo aplicar	Se entiende que la contribución al negocio está dada por el servicio cumplido. Existe responsabilidad mínima para garantizar que las medidas de respuesta son razonables y están en el lugar y reflejan el ambiente de amenazas y valor de activos. Las políticas de empresa y normas, pueden estar incompletas y/o reflejar solo las exigencias externas. Los eventos de TI	Los servicios se gestionan ad hoc, así como la recopilación de datos, métodos de análisis, los cuales son impulsados por evaluaciones ante un episodio determinado, así como el análisis de riesgos que puede existir sobre una base ad hoc y no se desarrolla activamente. Se identifican los riesgos y factores de riesgo pudiendo aplicar técnicas de gestión del conocimiento como cámaras web, videoconferencias y realidad virtual. Los respaldos de datos se realizan en forma esporádica, pudiendo existir un responsable de éstos, que debe estar claramente definido. La

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	aislada. El tiempo, recursos humanos y capacitación necesarios para el cumplimiento de las operaciones no está definido claramente a futuro.	técnicas y herramientas como redes, fusión y adquisición del conocimiento.	relacionados y condiciones que podrían afectar en el día a día las operaciones en ocasiones se discuten en reuniones de gestión, pero las respuestas de riesgo específico no se consideran. La socialización y externalización del conocimiento se desarrolla en forma aislada (islas de información), pudiendo utilizar herramientas de gestión del conocimiento como comunidades de práctica y grupos de expertos.	seguridad en TI es la intrínseca de las herramientas de software y hardware utilizadas, pudiendo existir autenticación y autorización (restricciones de acceso) de usuarios a través de contraseñas, así como el uso de firewall y antivirus.
Nivel 2: Gestionada y establecida	Se utilizan estándares definidos y comunicados para gestionar las operaciones actuales, adecuando los recursos a las arquitecturas, principios y necesidades futuras de TI. Los factores de tiempo, recursos humanos y económicos son definidos para la	Las operaciones deben satisfacer las necesidades de los distintos usuarios (internos y externos) de los servicios de TI. El conocimiento sobre riesgos, factores y respuesta al riesgo, se identifican,	Las operaciones deben cumplir con las necesidades del negocio, establecidas a través de las estrategias. Existe una comprensión individual sobre el impacto de las amenazas y acciones específicas a tomar en caso de que se	Se implementan estándares para gestionar la calidad de los servicios. Se implantan planes de capacitación para los RRHH de TI. Las competencias requeridas en cada área están definidas y documentadas, considerando la recopilación de datos, análisis de riesgo y perfiles. Se aplican las técnicas y herramientas de gestión del conocimiento que mejor

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	<p>gestión del conocimiento en la operativa. La gestión de riesgos de TI, factores y respuestas a riesgos, se desarrollan aplicando técnicas y herramientas apropiadas, como comunidades de práctica, redes y mejores prácticas. La organización define normas para la gestión de los riesgos y el conocimiento, con la participación activa del CKO.</p>	<p>adquieren y desarrollan haciendo uso de herramientas y técnicas de gestión del conocimiento como lecciones aprendidas y grupos de expertos. Los recursos humanos están comprometidos con el logro de la satisfacción de los usuarios.</p>	<p>concreten. Los responsables de las prácticas de respuesta al riesgo están definidos y los dueños de cada proceso están identificados. Se capacita al personal sobre riesgo en TI periódicamente, así como existe un plan de la organización y política para la respuesta al riesgo que definen cuando y como responder a los riesgos, el cual se desarrolla aplicando técnicas y herramientas de gestión del conocimiento como ser análisis de redes sociales, mapas de conocimiento y patentes, contando con el compromiso de la dirección para su logro.</p>	<p>se ajustan a la organización como ser sistemas expertos, redes, mejores prácticas y comunidades de práctica. El tiempo y recursos humanos para la capacitación están definidos, así como respaldos que se realizan periódicamente y que se almacenan fuera de la organización y testean regularmente. En los procesos críticos de la organización se realiza encriptación de datos. Existe un plan de recuperación de desastres que está definido informalmente, así como un plan de actualización regular de hardware y software.</p>
Nivel 3: Predecible	<p>Se mide la calidad de servicios y su capacidad futura. El análisis de riesgo es revisado y la causa de los problemas se investiga. Se desarrolla,</p>	<p>Se mide de acuerdo a los procesos definidos, la satisfacción de los usuarios del servicio. Se ha creado una conciencia</p>	<p>Se mide la contribución que realizan las operaciones de TI al negocio. Existe un líder de gestión del riesgo así como un líder de</p>	<p>Se mide y evalúa la eficiencia y eficacia de la gestión de riesgos y la respuesta al riesgo de forma cuantitativa. Se cuenta con una base común a toda la organización y se desarrolla, comparte y</p>

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	<p>capacita y forma al personal con planes a largo plazo en evaluación y gestión de riesgos. Se aplican herramientas de análisis de riesgo en base a un plan estándar, facilitado por el uso de herramientas y técnicas como e-learning y bases de conocimiento, guiados por marcos de buenas prácticas y recursos humanos capacitados en base a la cultura organizacional existente.</p>	<p>organizacional del riesgo por medio de la gestión del conocimiento y la aplicación de técnicas y herramientas como comunidades de práctica y grupos de expertos, por medio de la cual se ha aceptado la gestión del riesgo como una forma de comprender el estado de la organización frente a los riesgos, así como para alcanzar mejor los objetivos estratégicos de la organización.</p>	<p>gestión del conocimiento, comprometidos en su función, cuyos aportes generan valor para la toma de decisiones de la organización. Esta claramente definido el papel del departamento de TI en la gestión del riesgo operacional. El conocimiento es gestionado en todas sus etapas de externalización, interiorización, socialización y combinación, con el uso de herramientas y técnicas que mejor se ajustan.</p>	<p>usa el conocimiento, aplicando las técnicas y herramientas que mejor se ajustan a la operativa como charlas informales, contacto personal, coaching, mentoring y sistemas expertos. La organización realiza una gestión de los riesgos asociados a TI, contando con un plan de recuperación de desastres formalmente definido, así como medidas de seguridad física (control de acceso, sistemas de vigilancia, sistemas de prevención de desastres) aplicados a TI. Se utilizan certificados digitales y sistemas de PKI.</p>
Nivel 4: Optimizada	<p>Las capacidades (físicas, humanas, etc.) se han establecido para poder satisfacer las necesidades actuales y futuras. Se capacita los recursos humanos de forma sistemática y planificada. Se mide y se mejora la gestión del riesgo y el conocimiento, aplicando técnicas y herramientas</p>	<p>Las operaciones están orientadas a las necesidades de los usuarios. La empresa exige la mejora continua en la gestión de las capacidades de los riesgos de TI basada en objetivos claramente definidos de personal y de organización,</p>	<p>Los servicios aportan el valor esperado al negocio. Los objetivos estratégicos se basan en un entendimiento a nivel ejecutivo de las amenazas de negocios relacionados, los escenarios de riesgo y la competitividad de las oportunidades. Las políticas de</p>	<p>Los servicios son optimizados de forma de maximizar el valor que aportan al negocio. Existe seguimiento en tiempo real de los eventos y excepciones de control al igual que la automatización de la gestión. Las estrategias de respuesta de riesgo son aplicadas de manera integral y cuando sea plenamente justificado, controles costo-eficacia mitigan la exposición al riesgo en forma continua. La empresa exige</p>

	Proyección de futuro	Orientación al usuario	Contribución al negocio	Excelencia operativa
	<p>como mentoring, coaching, charlas informales, grupos de expertos. Los líderes de gestión del riesgo y conocimiento son considerados asesores de confianza en el diseño e implementación de operaciones. La alta gerencia considera en sus decisiones todos los aspectos de la gestión del riesgo y conocimiento, haciendo uso y mejorando la memoria organizacional, con el uso de marcos de buenas prácticas a través de una cultura organizacional en gestión del conocimiento en riesgo.</p>	<p>que se logra aplicando técnicas y herramientas de gestión del conocimiento como coaching, mentoring, charlas informales y contacto personal. Las respuestas a los riesgos reales en las operaciones se comunican en toda la empresa. El conocimiento se distribuye y usa, por medio de técnicas y herramientas como mapas de conocimiento, accesibilidad y diseño del área de trabajo.</p>	<p>empresa y las normas siguen reflejando la tolerancia al riesgo empresarial mientras aumenta la eficiencia. La empresa exige formalmente la mejora continua de la gestión de las capacidades de los riesgos de TI basada en objetivos claramente definidos de personal y de organización. Los responsables de las decisiones cuentan con la mejor información sobre probabilidades de pérdida, riesgos y oportunidades a través del correcto uso, desarrollo y distribución del conocimiento, mejorado por la aplicación de técnicas y herramientas como benchmarking, mentoring, coaching, charlas informales.</p>	<p>formalmente la mejora continua de las capacidades de respuesta de riesgos sobre la base de definir claramente los objetivos personales y de organización. Las herramientas automatizadas permiten de inicio a fin, el apoyo y la mejora de los esfuerzos de evaluación de riesgos. Se aplican sistemáticamente técnicas y herramientas que permiten gestionar el conocimiento en todas sus etapas, por medio de una base organizacional, haciendo uso de técnicas y herramientas de gestión del conocimiento como clustering, clasificación y sistemas expertos. Se cuenta con un plan de continuidad del negocio aplicado a TI, así como la aplicación de un conjunto estandarizado de buenas prácticas para la gestión de riesgos asociados a TI y se asignan responsabilidades claramente definidas para cada riesgo identificado.</p>

Anexo XVI – Indicadores para el Modelo de Gestión del Riesgo basado en la Gestión del Conocimiento

1.0 Gestión del Riesgo - Indicadores

1.1 Gestión del Riesgo Proceso Gobierno del Riesgo (RG)

RG 1 – Establece y mantiene una visión de riesgo común

RG 1.1 - Desarrollar en una empresa el marco específico de gestión de riesgos de TI

Categoría Básica

1. Porcentaje de variables de negocio para las cuales se ha identificado y registrado los puntos de TI que pueden aportar valor al negocio, para los cuales existe un análisis de tolerancia al riesgo.
2. Existencia de mapas de conocimiento que vinculan los eventos de TI identificados.

RG 1.2 – Proponer los umbrales de tolerancia de riesgos de TI

Categoría Básica

1. Porcentaje de procesos de negocio que cuentan con medidas de riesgo y niveles de tolerancia asociados.

Categoría Avanzada

2. Nro de medidas realizadas por proceso de negocio.

RG 1.3 – Aprobar la tolerancia al riesgo

Categoría Básica

1. Existencia de mapas de conocimiento y base de conocimiento de todas las áreas de la empresa con umbrales de riesgo por área de negocio.

RG 1.4 – Alinear la política de riesgos de TI

Categoría Básica

1. Existencia de base de conocimiento de la organización con apetito al riesgo y tolerancia de cada área de negocio.

Categoría Avanzada

2. Nro de horas de reunión de grupos de expertos por cada área sobre el número de áreas de negocio de la empresa, dedicados a la definición del apetito y tolerancia al riesgo de cada área.

RG 1.5 – Promover los riesgos de TI – cultura consciente

Categoría Básica

1. Nro de cursos por horas dedicadas sobre nro de personas capacitadas en gestión del riesgo para cada área de negocio.
2. Existencia de base de conocimientos con registro de acciones y buenas prácticas en gestión del riesgo de cada área de negocio.
3. Existencia del rol CKO dedicado a la comunicación de la política de gestión del riesgo en la organización.
4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.

RG 1.6 – Promover una comunicación efectiva de los riesgos de TI

Categoría Básica

1. Existencia de un plan de comunicación de riesgos
2. Existencia de una base de conocimiento organizacional accesible por responsables y directores con información sobre amenazas e impacto de riesgos por área.
3. Nro de amenazas por área de negocio de la base de conocimiento.
4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.
5. Nro de reuniones del CKO con los distintos responsables de cada área de la empresa, dedicadas a la comunicación de la política de gestión del riesgo en la organización.

RG 2 – Integrar con ERM

RG 2.1 – Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa

Categoría Básica

1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes.

Categoría Avanzada

2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno.

RG 2.2 – Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial

Categoría Básica

1. Cursos por horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos.
2. Nro de reuniones por horas dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos.
3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos.

RG 2.3 - Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa

Categoría Básica

1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.
2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.
3. Horas de capacitación o reuniones de recursos de la empresa, sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo.

RG 2.4 - Proporcionar recursos adecuados para la gestión de riesgos

Categoría Básica

1. Nro de horas en capacitación al personal de cada área en gestión del riesgo sobre total de recursos humanos del área.
2. Existencia de una base de conocimiento de la organización y mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.

RG 2.5 - Garantizar el aseguramiento independiente sobre la gestión de riesgos

Categoría Básica

1. Existe una base de conocimiento con el registro del apetito al riesgo y tolerancia que permite la gestión del riesgo por parte del director de TI y director general.
2. Existencia de mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.

Categoría Avanzada

3. Horas en capacitación de recursos humanos asegurando su independencia en la gestión de riesgos.

RG 3 – Toma de decisiones consciente del riesgo de negocios

RG3.1 - Ganancia de la gestión de compra para el enfoque de análisis de riesgos

Categoría Básica

1. Existe una base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo.
2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.
4. Horas de capacitación en concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos de la empresa.

Categoría Avanzada

3. Horas de capacitación o reuniones que permitan interpretar los informes de análisis de riesgo y brechas existentes con el riesgo empresarial.

RG 3.2 - Aprobar el análisis de riesgos de TI

Categoría Básica

1. Existe una base de conocimiento única para las distintas áreas de la empresa accesible a todos los directores de área que permite registrar, transmitir y usar dicho conocimiento.
2. Nro de horas en capacitación y reuniones para la formación de los directores de área en la cultura de gestión del riesgo a través de la gestión del conocimiento.

RG 3.3 - Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio

Categoría Básica

1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.
2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.

3. Horas de capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio.

RG 3.4 - Aceptar los riesgos de TI

Categoría Básica

1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.
2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.

Categoría Avanzada

3. Horas de capacitación en formación al personal sobre aceptación y gestión del riesgo de TI para el negocio de cada área de la empresa.

RG 3.5 - Priorizar actividades de respuesta de riesgos de TI

Categoría Básica

1. Existe una base de conocimiento para la gestión del riesgo en la empresa disponible para el director general y director de TI, que permita registrar métricas para el seguimiento del cumplimiento de las actividades de TI, así como priorización de las mismas, con información sobre el apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles.
2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.
3. Horas de capacitación y formación al director general y de TI sobre seguimiento y planificación de riesgos en TI.

1.2 Gestión del Riesgo Proceso Evaluación del Riesgo (RE)

RE 1.1 - Establecer y mantener un modelo para la recolección de datos

Categoría Básica

1. Existe apoyo explícito de la dirección para la concreción de la recopilación de datos para la formación de un repositorio único de conocimiento, así como en la culturización en gestión del conocimiento en la empresa.
2. Existe una estrategia de adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.
4. Horas de capacitación y formación realizadas con el personal de la empresa respecto a la recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento en la organización.

Categoría Avanzada

3. Existe una implementación para la adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.

RE 1.2 - Recopilar datos sobre el entorno externo

Categoría Básica

1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.

RE 1.3 - Recopilar datos sobre eventos de riesgo

Categoría Básica

1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.

Categoría Avanzada

2. Nro de incidencias registradas sobre riesgos detectados en eventos históricos sobre experiencias propias y de terceros disponibles en la base de conocimiento organizacional sobre gestión de riesgos.

RE 1.4 - Identificar factores de riesgo

Categoría Básica

1. Horas de reuniones de charlas con expertos, coaching, comunidades de práctica realizadas por directivos de TI y de las restantes áreas de la empresa, aplicadas para la identificación de riesgos, asociados a proyectos, programas, servicios existentes y futuros, etc. que pueden generar eventos de riesgo.

2. Existencia de una base de conocimiento organizacional donde se integra información sobre proyectos, programas, servicios e incidentes.

Categoría Avanzada

3. Nro de relaciones entre factores de riesgo identificados que se relacionan entre sí en la base de conocimiento organizacional, sobre el total de los mismos.

RE 2.1 - Definir Alcance del Análisis de Riesgo

Categoría Básica

1. Horas de capacitación y formación al personal responsable de la gestión del riesgo y del negocio de la empresa, en cuanto a gestión y evaluación del riesgo.

Categoría Avanzada

2. Horas de reuniones de charlas con expertos, benchmarking, realizadas con el personal responsable de la gestión del riesgo y el negocio sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo de la organización.

RE 2.2 - Estimación de riesgos en TI

Categoría Básica

1. Horas de capacitación y formación a los responsables del riesgo y de negocio de la empresa, sobre análisis de información de riesgo (factores, frecuencia, magnitud y tolerancia al riesgo) para la estimación y definición de controles.

2. Existencia de un CMS disponible para el análisis en la estimación de riesgos.

Categoría Avanzada

3. Horas de reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos.
4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos en el CMS de la empresa.

RE 2.3 - Identificar las opciones de respuesta de riesgo

Categoría Básica

1. Horas de capacitación y formación a los directivos y responsables del riesgo sobre identificación de respuestas de riesgo.
2. Existencia de un CMS disponible para la consulta y actualización de respuestas de riesgo.
3. Horas de reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos.

Categoría Avanzada

4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas de riesgos en el CMS de la empresa.

RE 2.4 - Realizar una revisión por pares de los resultados de análisis de riesgos de TI

Categoría Básica

1. Horas de capacitación y formación a los responsables del riesgo sobre la aplicación de técnicas para el análisis de riesgos de TI.
2. Existencia de un CMS disponible para la actualización de la información sobre riesgos de TI en la empresa.
3. Horas de reuniones de charlas con expertos, charlas formales e informales, coaching en asignación de recursos.

Categoría Avanzada

4. Aplicación de sistemas expertos en la resolución de la asignación de recursos.

RE 3.1 - Mapa de recursos de TI para procesos de negocio

Categoría Básica

1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.
3. Horas de capacitación y formación a los responsables del riesgo en la empresa, sobre uso y análisis de mapas de conocimiento.

RE 3.2 - Determinar la criticidad de negocios de los recursos de TI

Categoría Básica

1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.
2. Horas de capacitación y formación a los responsables de la gestión de los recursos en las distintas áreas de la empresa, sobre la determinación de criticidad de los recursos según los requerimientos de la organización.

3. Horas de reuniones de charlas con expertos, charlas formales e informales para la definición de la criticidad de los recursos de TI en cada área.
4. Existencia de un CMS con información sobre riesgos, recursos y su criticidad.

RE 3.3 - Entender las capacidades de TI

Categoría Básica

1. Horas de capacitación y formación de los responsables de TI y responsables de cada área, para la evaluación de las capacidades disponibles y análisis de situación.
2. Existe plan de capacitación de los responsables de cada área y de TI, sobre gestión del riesgo de TI.
3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.
4. Existencia de un CMS con información sobre las capacidades y requerimientos en TI de la empresa.

Categoría Avanzada

5. Horas de reuniones de charlas formales e informales, consultas a expertos, sobre análisis de las capacidades existentes en TI y sus requerimientos.

RE 3.4 - Actualización de los componentes del escenario de riesgos de TI

Categoría Básica

1. Horas de capacitación y formación de los responsables de negocio, riesgo y TI, para la evaluación de escenarios de riesgo.
2. Existencia de un CMS con información sobre riesgos y distintos escenarios de riesgo.

Categoría Avanzada

3. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre análisis de distintos escenarios de riesgo.

RE 3.5 - Mantener los riesgos de TI y mapa de registro de riesgos de TI

Categoría Básica

1. Horas de capacitación y formación de los responsables de negocio y TI, para la actualización de riesgos de TI y definición de perfil de riesgo.
3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.

Categoría Avanzada

2. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre definición de perfil de riesgo de la organización.

RE 3.6 - Diseñar y comunicar los indicadores de riesgo de TI

Categoría Básica

1. Existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo en TI en la empresa.

2. Horas de reuniones de charlas formales y consultas a expertos sobre difusión de indicadores de riesgo de la empresa.

Categoría Avanzada

3. Existencia de conocimiento actualizado sobre buenas prácticas en difusión de indicadores en la base de conocimiento de la empresa.

1.3 Gestión del Riesgo Proceso Respuesta del Riesgo (RR)

RR 1.1 - Informe de los resultados de análisis de riesgos de TI

Categoría Avanzada

1. Horas de reuniones de charlas formales, consultas a expertos, coaching, mentoring sobre gestión de la comunicación.

Categoría Básica

2. Horas de capacitación y formación sobre técnicas y herramientas de comunicación y coordinación.

3. Existe un CMS a nivel de la organización que permite adquirir el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, por parte de los responsables de negocio, riesgo y directores.

RR 1.2 - Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento

Categoría Avanzada

1. Horas de reuniones de charlas formales e informales, consultas a expertos, coaching, mentoring sobre generación de informes y comunicación.

Categoría Básica

2. Existe un CMS a nivel de la organización que permite la distribución de la información estratégica resultado de la gestión de riesgos.

3. Existencia de conocimiento actualizado en el CMS sobre lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados.

RR 1.3 - Interpretar resultados de la evaluación independiente de TI

Categoría Básica

1. Existencia de conocimiento actualizado en el CMS para el análisis de acciones correctivas e identificación de oportunidades de mejora.

2. Horas de capacitación y formación de recursos humanos de la empresa en el análisis del conocimiento del CMS para la generación de planes de acción correctiva.

3. Existencia de un plan de acción correctiva

Categoría Avanzada

4. Horas de reuniones de charlas formales e informales, contacto personal, mentoring sobre el análisis de acciones correctivas y mejoras en la gestión del riesgo.

RR 1.4 - Identificar TI – Oportunidades relacionadas

Categoría Básica

1. Horas de capacitación y formación de recursos humanos responsables de TI y del negocio de la empresa en el análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI.

Categoría Avanzada

2. Horas de reuniones de charlas con expertos, coaching, benchmarking sobre optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas.

RR 2.1 - Controles del inventario

Categoría Básica

1. Existencia de conocimiento actualizado en el CMS para el control de inventario de riesgos.

2. Horas de capacitación y formación de recursos humanos de la empresa en el control de inventarios de riesgo y clasificación de controles.

Categoría Avanzada

3. Horas de reuniones de charlas formales e informales, coaching y mentoring sobre control del riesgo.

RR 2.2 - Supervisar la alineación operacional de los umbrales de tolerancia al riesgo

Categoría Básica

1. Existe apoyo explícito de la dirección en la definición de indicadores de riesgo y definición de umbrales de tolerancia al riesgo.

2. Existe un CMS de la organización con riesgos, tolerancia al riesgo y umbrales, disponible para la supervisión de la alineación operacional de los umbrales a la tolerancia al riesgo.

3. Existen reuniones de charlas y grupos de expertos para el logro de la aceptación de indicadores por parte de las áreas operativas y dirección.

4. Horas de capacitación a la dirección en la definición de umbrales de tolerancia al riesgo y supervisión.

RR 2.3 - Responder a la exposición al riesgo descubierto y la oportunidad

Categoría Básica

1. Existencia de conocimiento actualizado en el CMS para la respuesta al riesgo.

3. Existencia de un mapa de conocimiento que facilite el acceso y distribución de los riesgos descubiertos y oportunidades.

Categoría Avanzada

2. Horas de reuniones de charlas formales e informales, coaching, mentoring sobre respuestas al riesgo **descubierto y oportunidades**.

RR 2.4 - Implementar los controles

Categoría Básica

1. Existe un CMS actualizado con el conocimiento sobre controles de riesgo.
3. Existencia de un mapa de conocimientos actualizado que cuenta con la distribución del riesgo y controles existentes en la organización.
4. Horas de capacitación y formación en la implementación de controles y uso de mapas de conocimiento para el mismo.

Categoría Avanzada

2. Horas de reuniones de coaching, mentoring, charlas formales e informales, sobre implementación de controles.

RR 2.5 - Informe del progreso del plan de acción de riesgos de TI

Categoría Básica

1. Horas de capacitación al personal de TI y responsables del riesgo, en supervisión del plan de acción.
3. Horas de reuniones destinadas a la comunicación sobre el progreso del plan de acción.

Categoría Avanzada

2. Horas de reuniones de charlas, grupos de expertos, benchmarking en supervisión del plan de acción.

RR 3.1 - Mantener los planes de respuesta a incidentes

Categoría Básica

1. Existe un CMS actualizado de respuestas a incidentes, accesible a los responsables de TI y gestión del riesgo.
2. Horas de reuniones en charlas, grupos de expertos sobre comunicación y gestión de planes de respuesta.

RR 3.2 - Supervisión de riesgos de TI

Categoría Básica

1. Horas de capacitación a responsables del riesgo y auditores sobre supervisión de riesgo de TI.
2. Existencia de un CMS sobre riesgos y límites de la organización accesible a los responsables del riesgo y auditores.

Categoría Avanzada

3. Horas de reuniones con grupos de expertos, charlas formales e informales sobre mejora en los riesgos de TI en base a los riesgos y límites tolerados.

RR 3.3 - Iniciar planes de respuesta a incidentes

Categoría Básica

1. Horas de capacitación y formación de responsables de la gestión y el riesgo de la empresa, en el logro de las mejores respuestas de cada incidente y el uso del CMS de la organización para ello.
3. Existencia de una base de conocimiento actualizada con categorías de hechos y respuestas.

Categoría Avanzada

2. Horas de reuniones en charlas formales e informales y benchmarking para lograr las mejores respuestas a incidentes y correcta distribución del conocimiento a los interesados.

RR 3.4 - Comunicar las lecciones aprendidas de eventos de riesgo

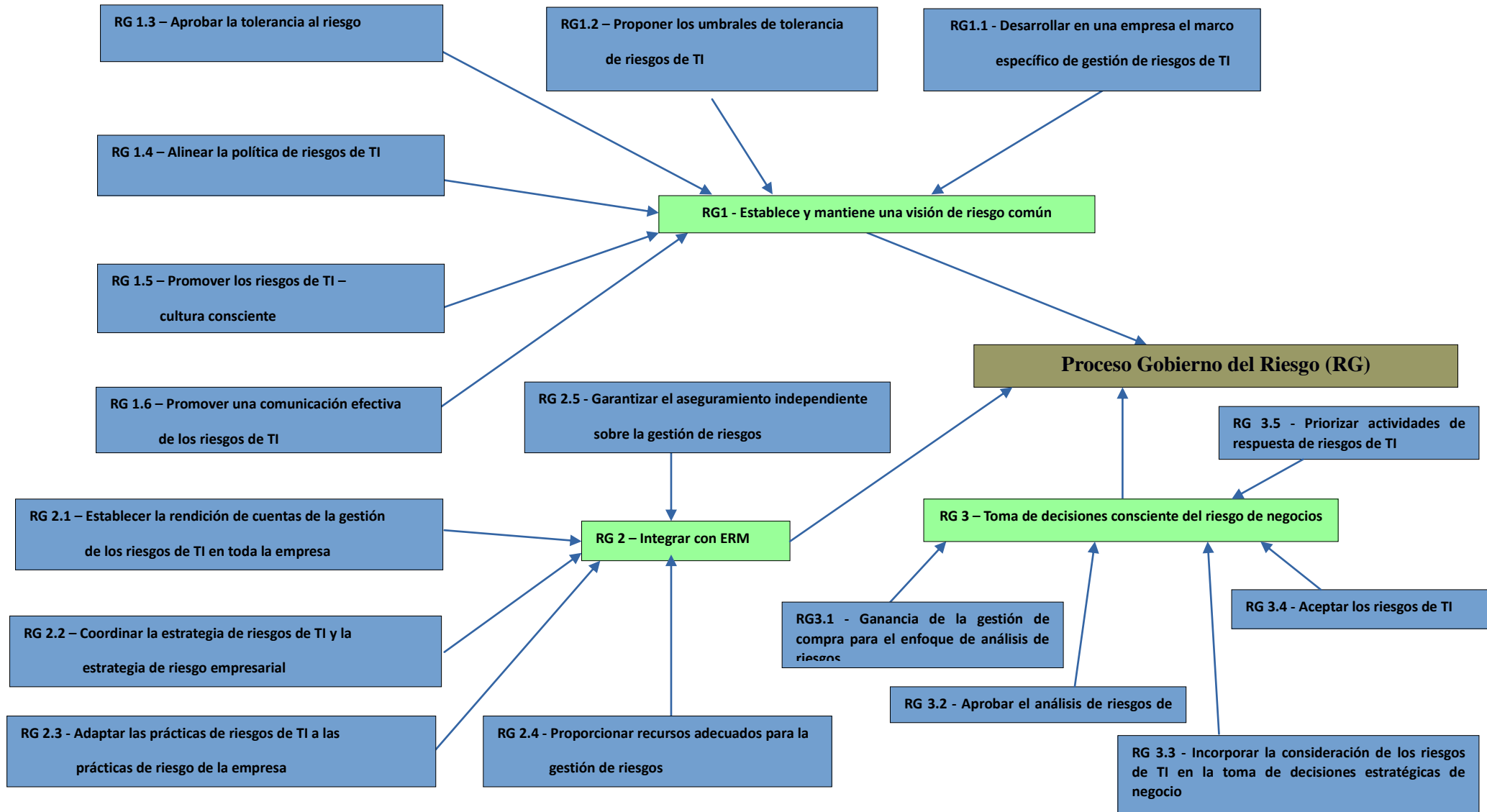
Categoría Básica

1. Horas de capacitación y formación de responsables de TI y del riesgo de la empresa, en la identificación de las causas de problemas.
3. Existencia de un CMS actualizado con datos históricos y recientes de acontecimientos adversos y pérdidas.

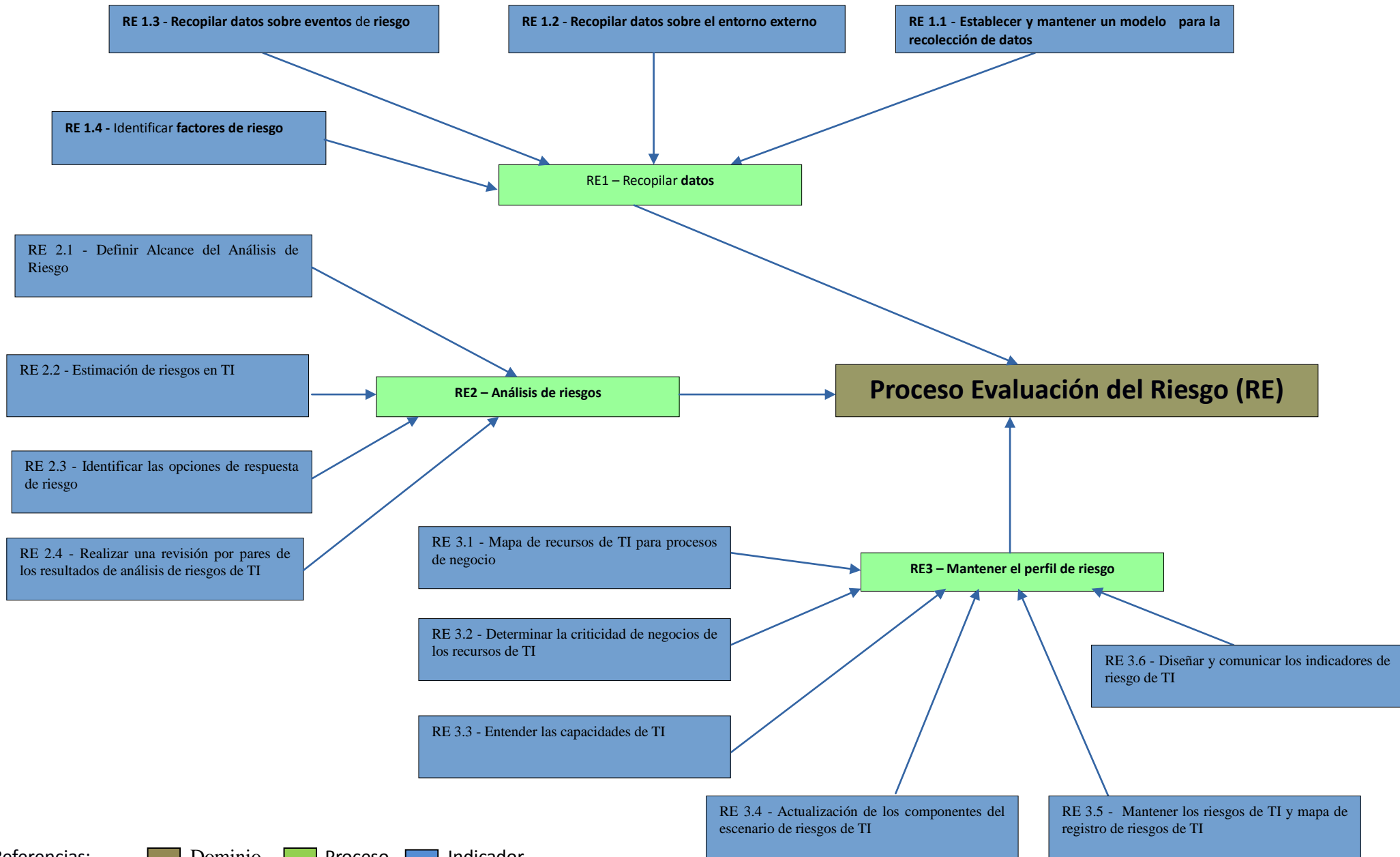
Categoría Avanzada

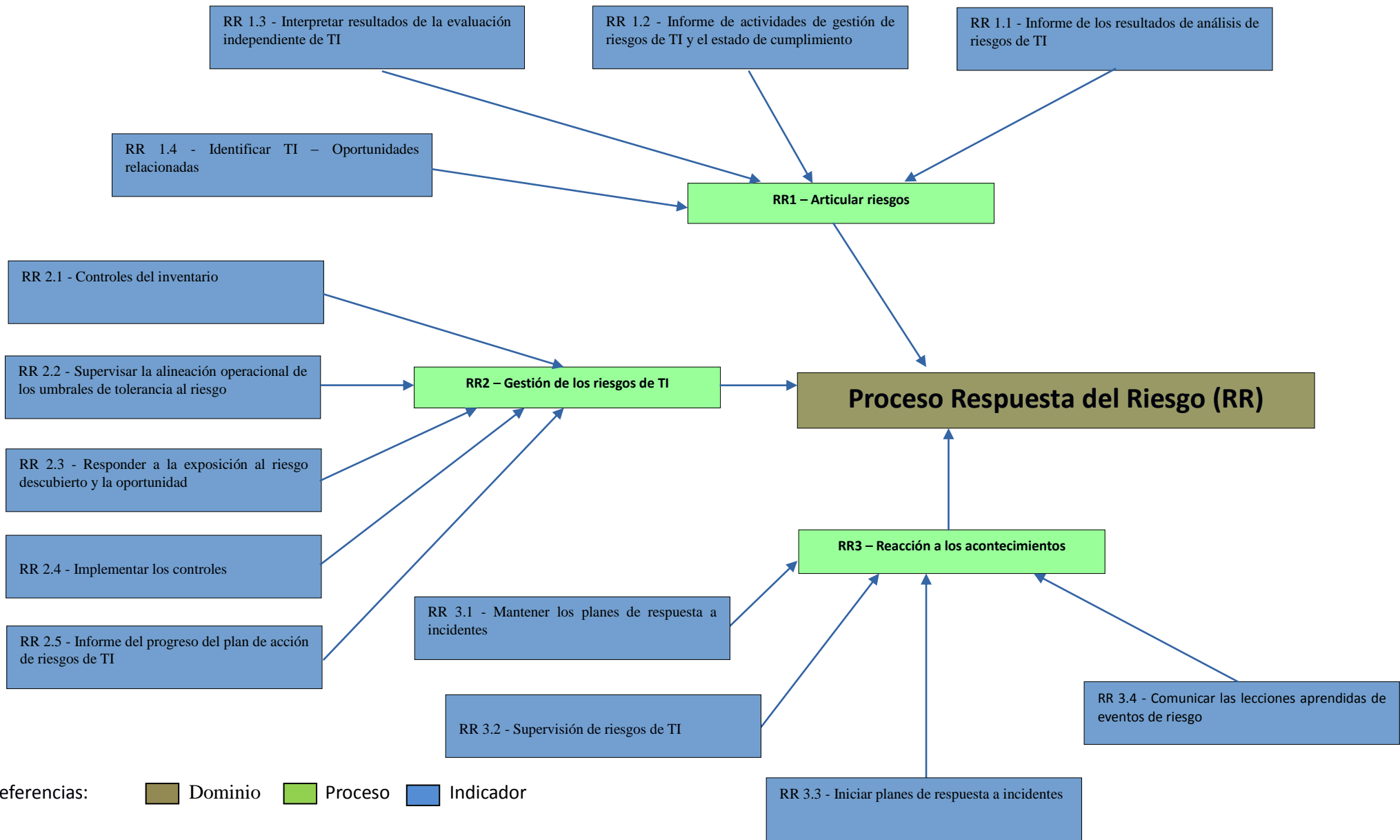
2. Horas de capacitación en charlas, grupos de expertos y benchmarking sobre identificación de causas de problemas.

Relación: Dominio / Proceso / SubProceso

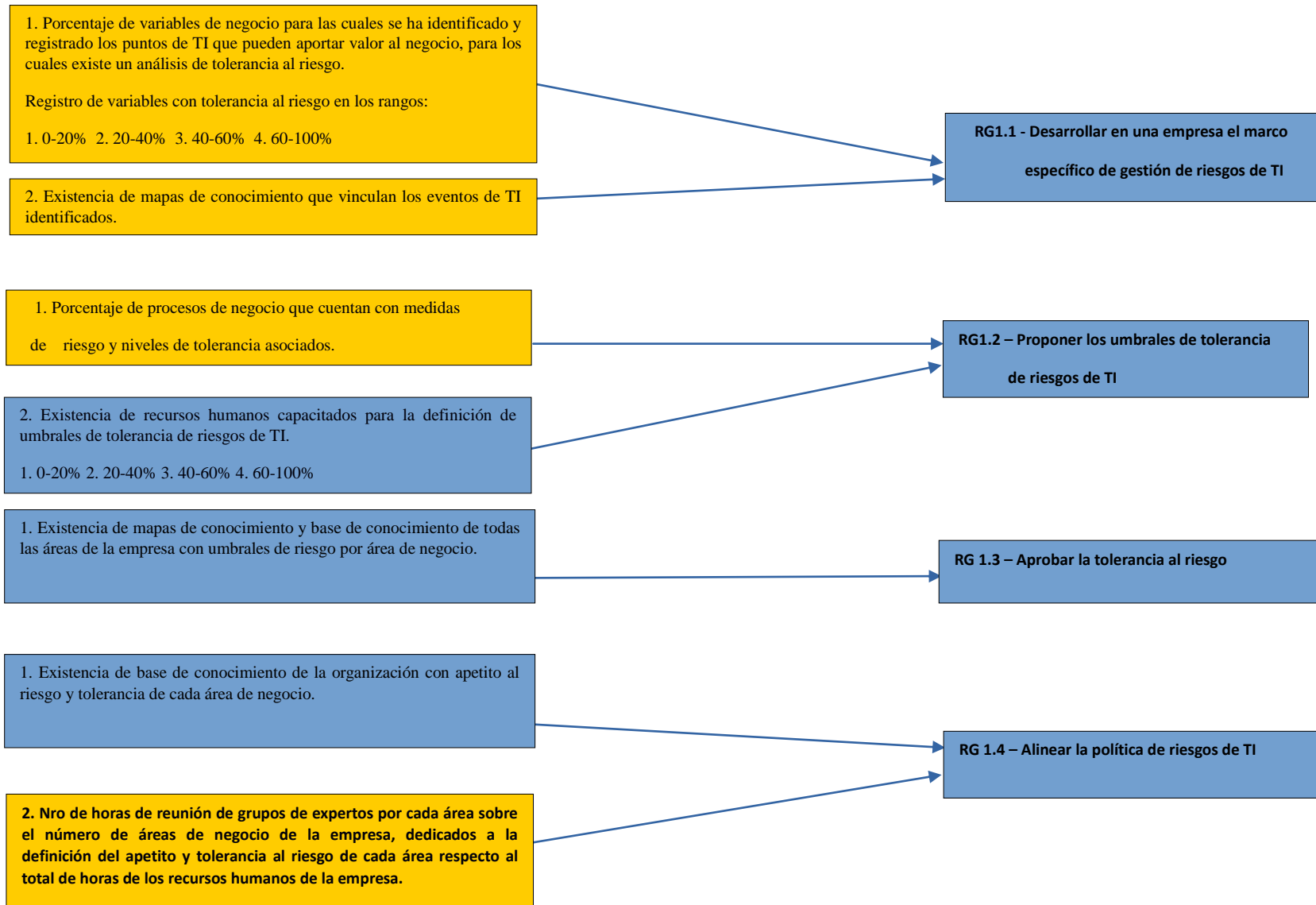


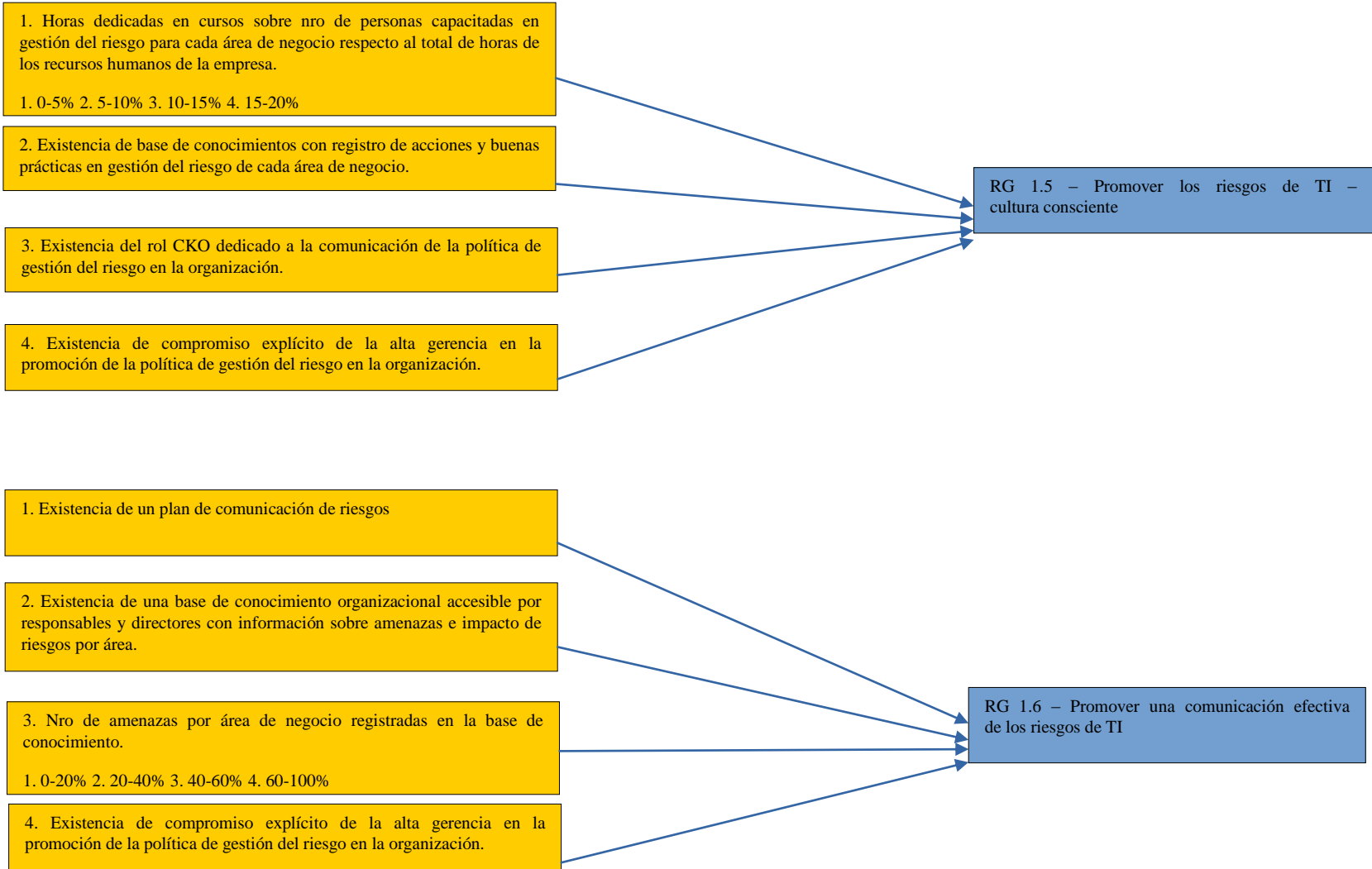
Referencias: Dominio Proceso Indicador





Relación: SubProceso / Indicadores (Referencia: ■ Básicos ■ Avanzados)





1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes.

2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno.
1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%

RG 2.1 – Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa

1. Horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa.
1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%

2. Horas de reuniones dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa.
1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%

RG 2.2 – Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial

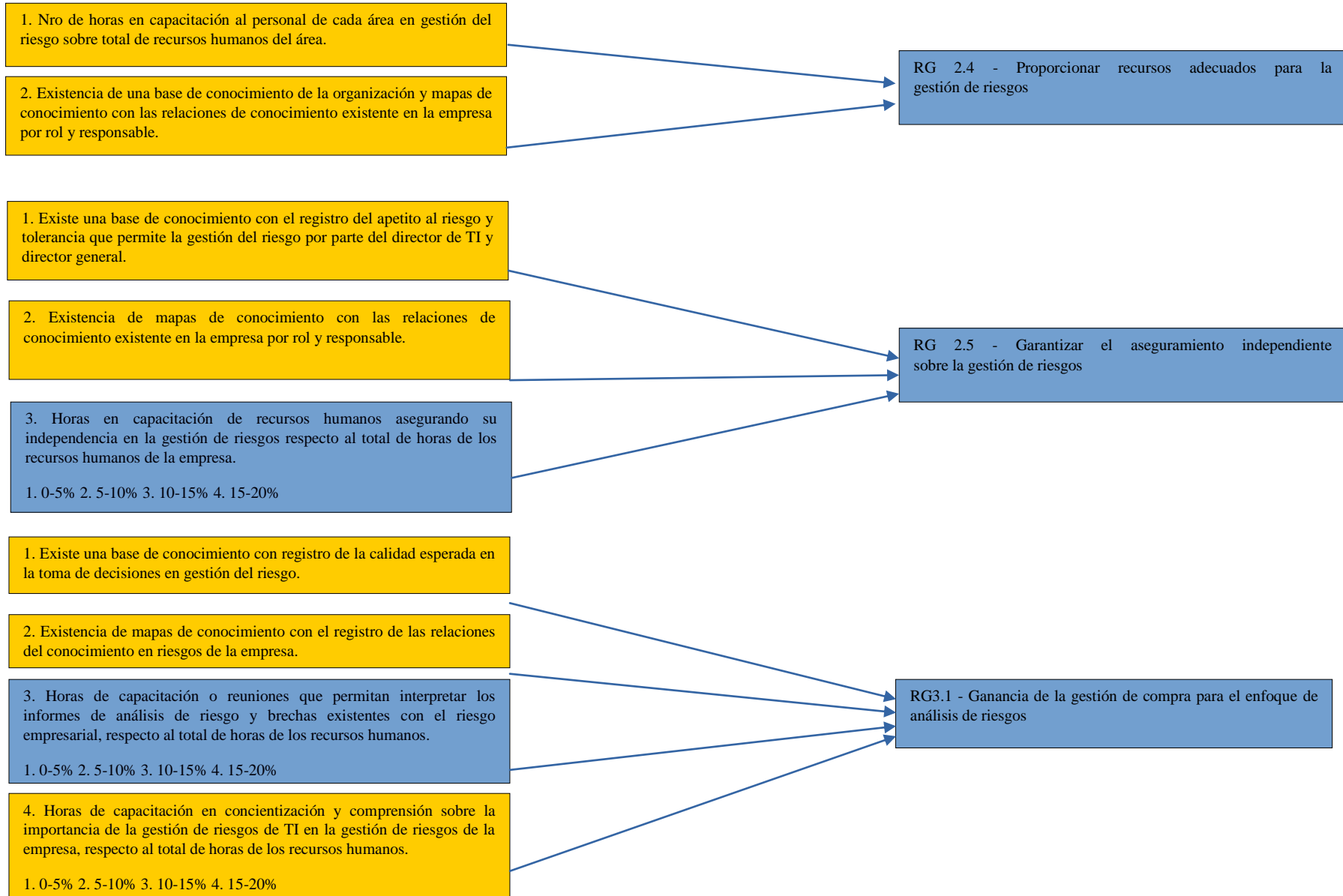
3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos.
1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%

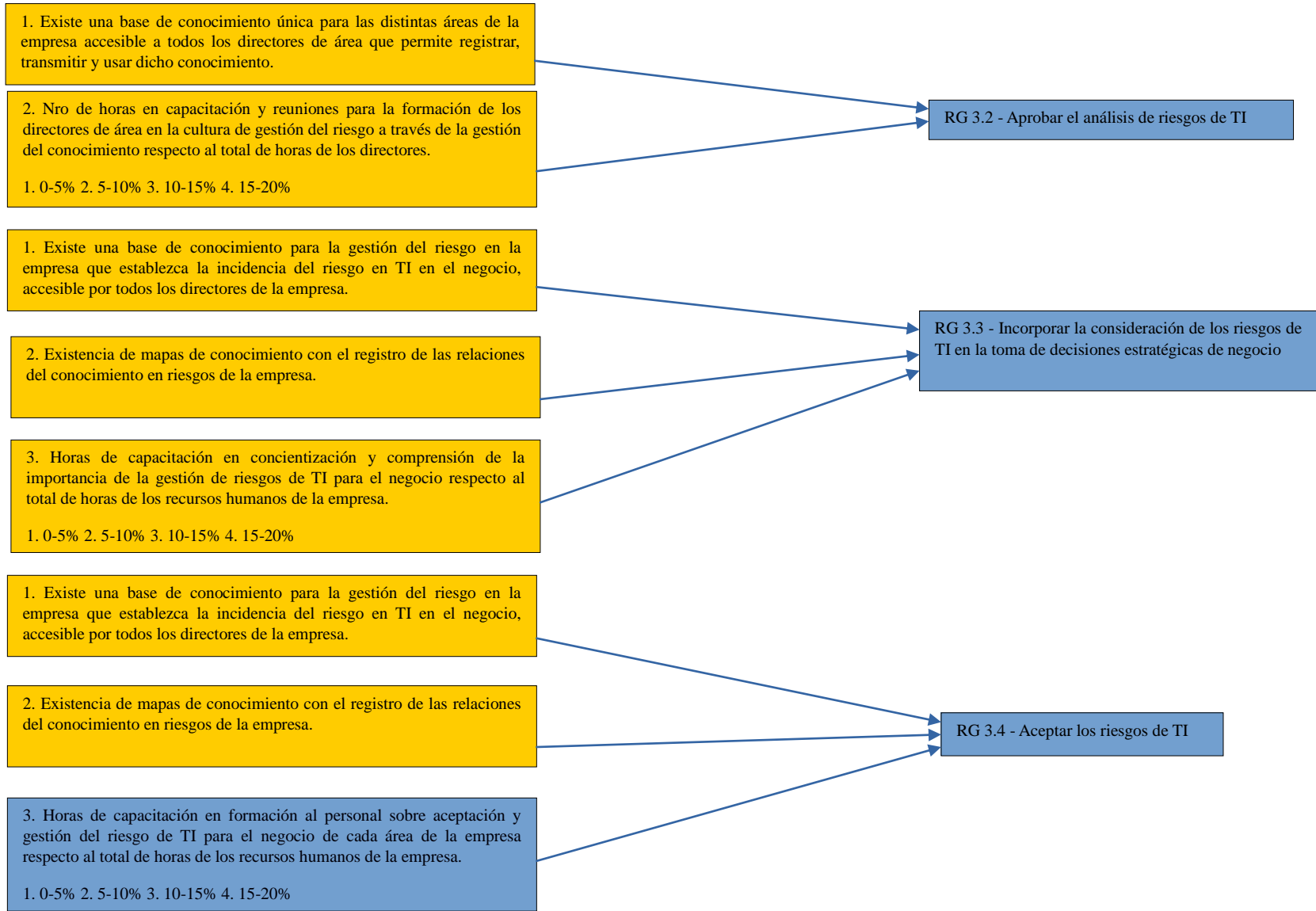
1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.

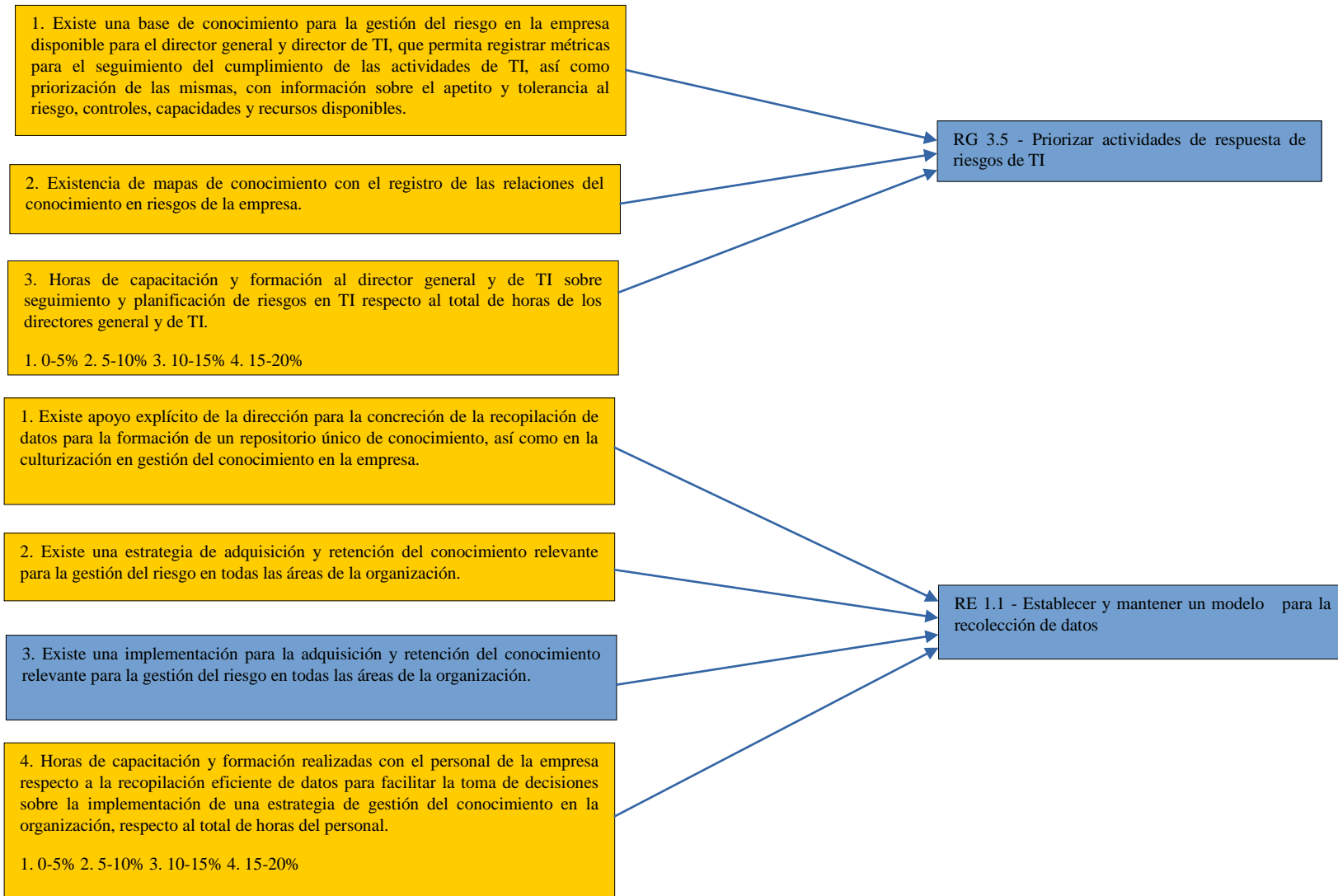
2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.

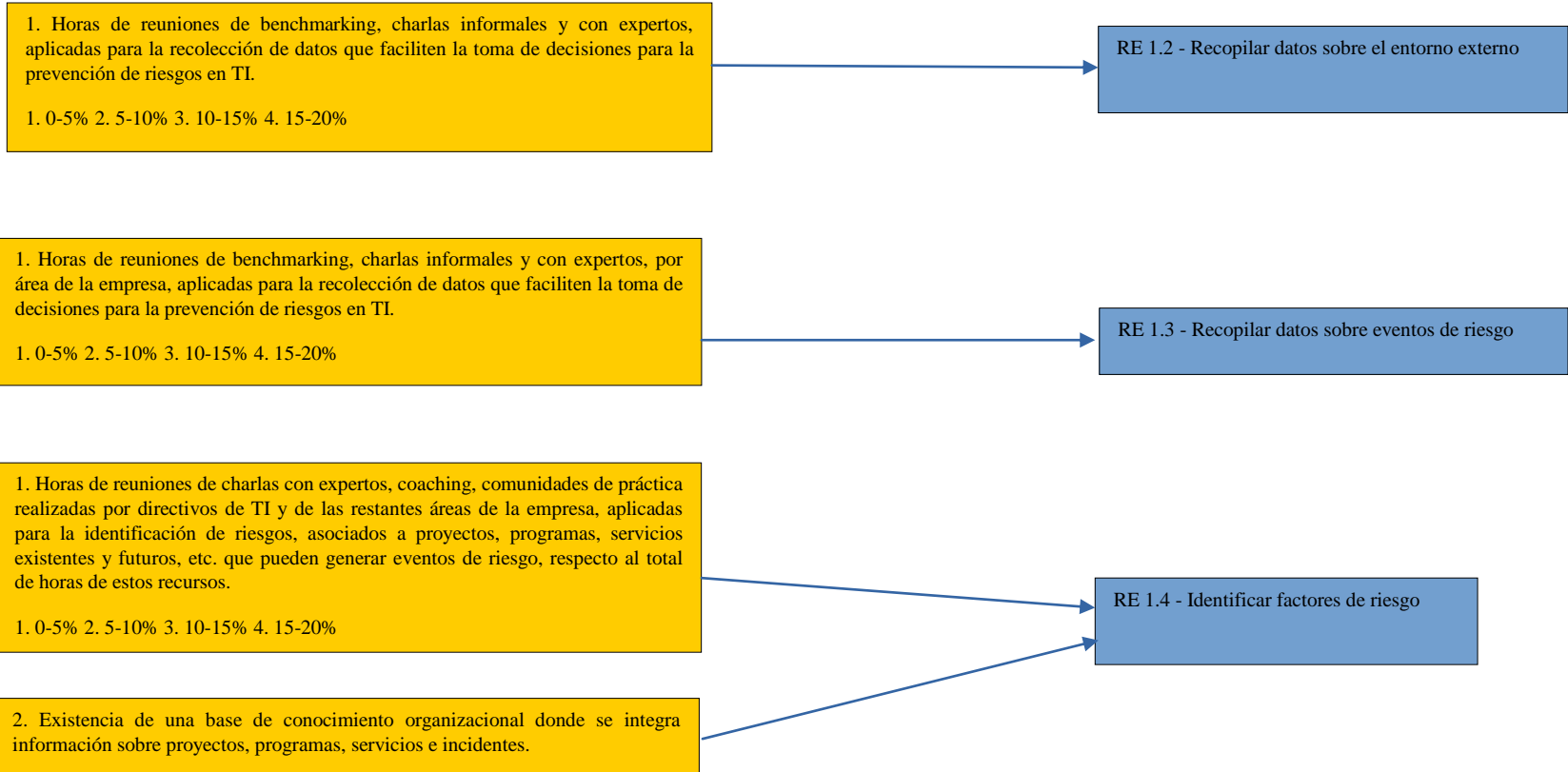
3. Porcentaje de recursos de la empresa capacitados o que asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo.
1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%

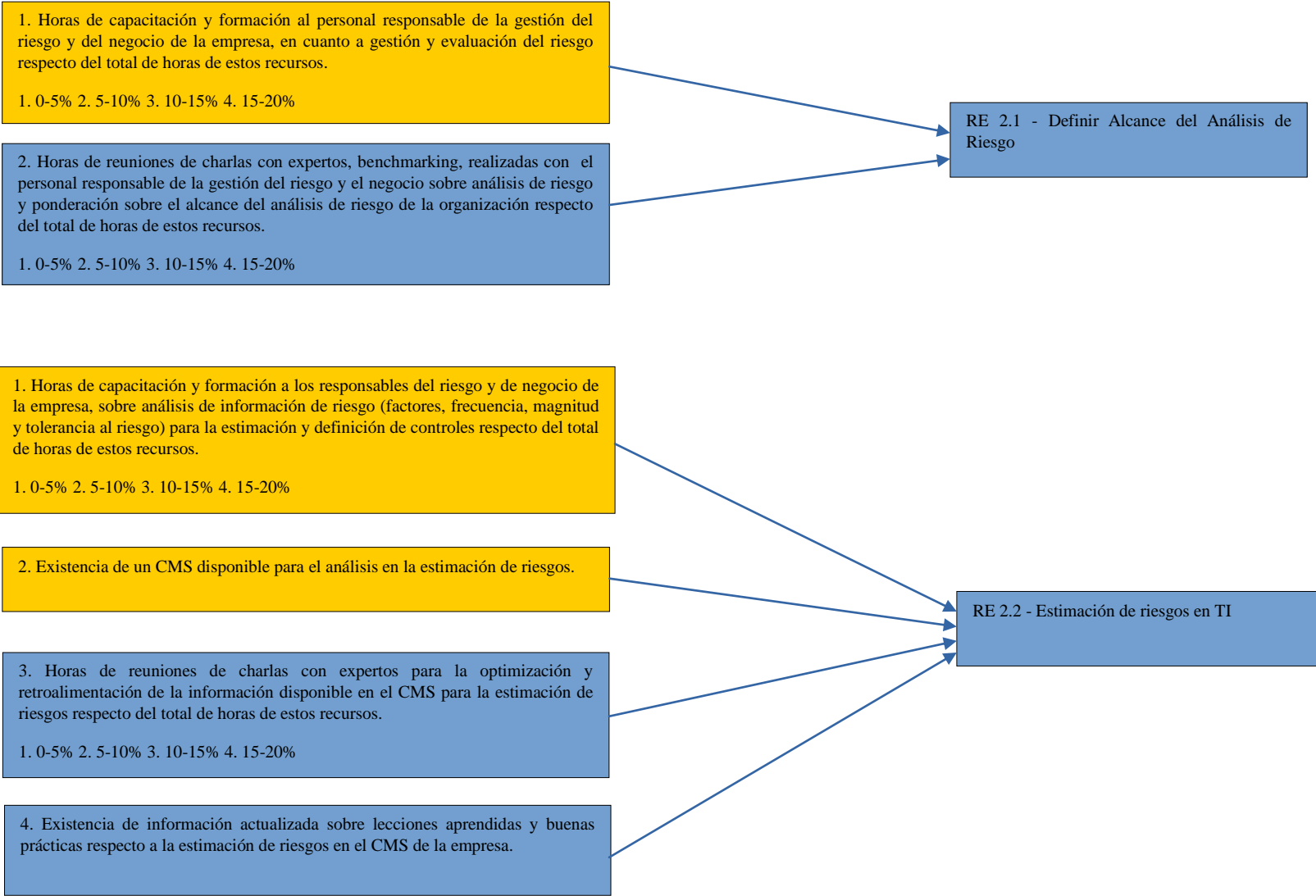
RG 2.3 - Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa

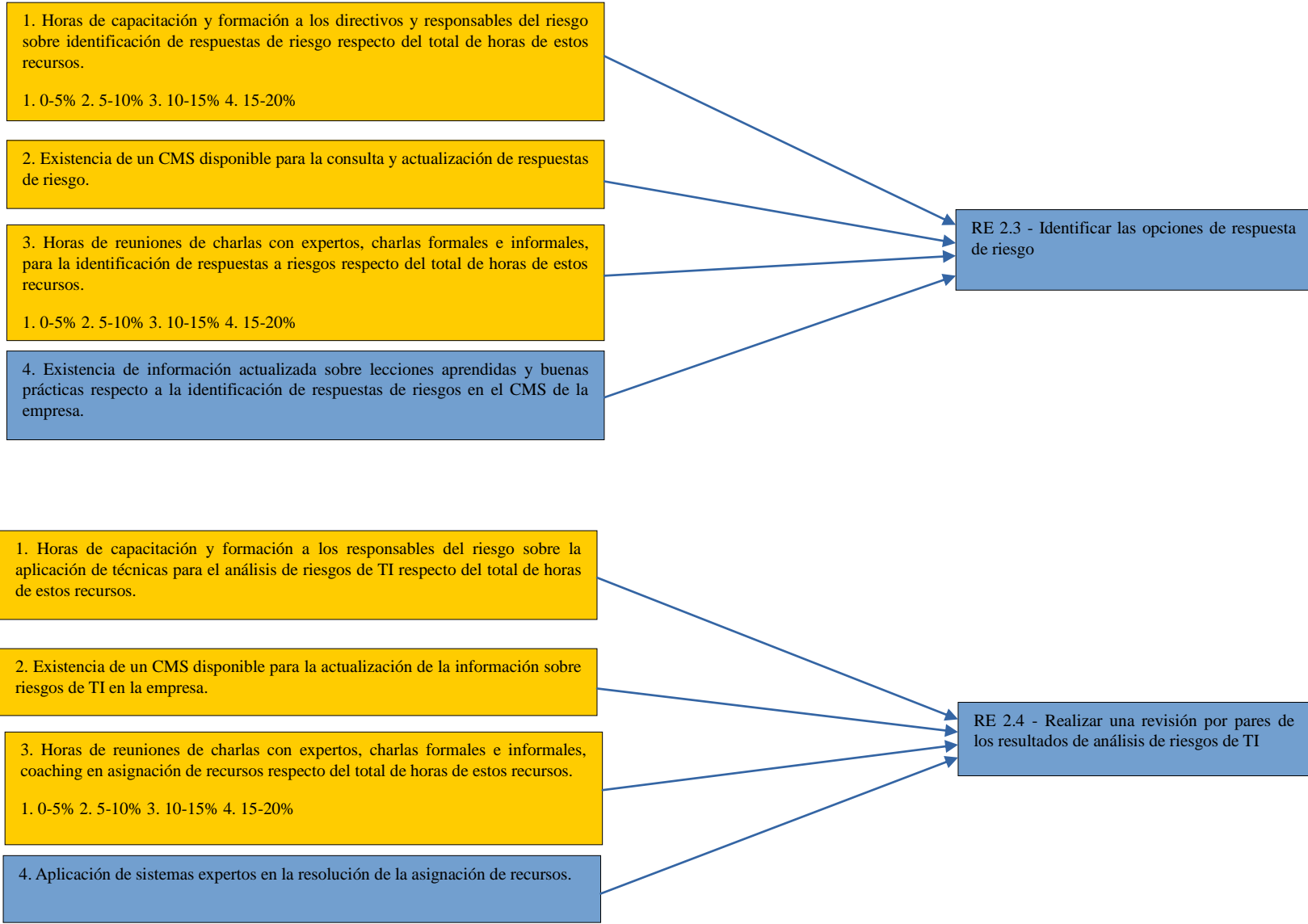


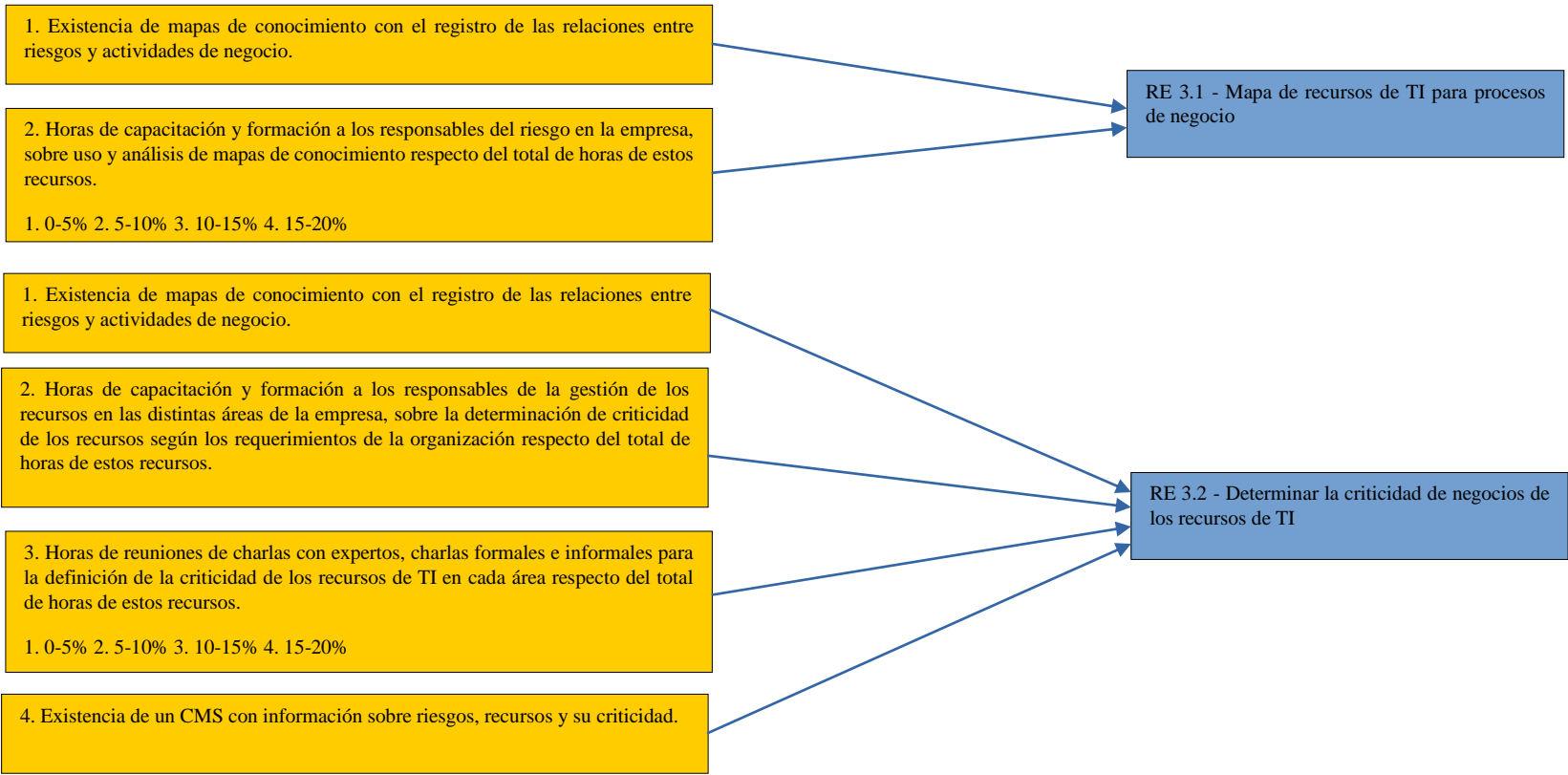


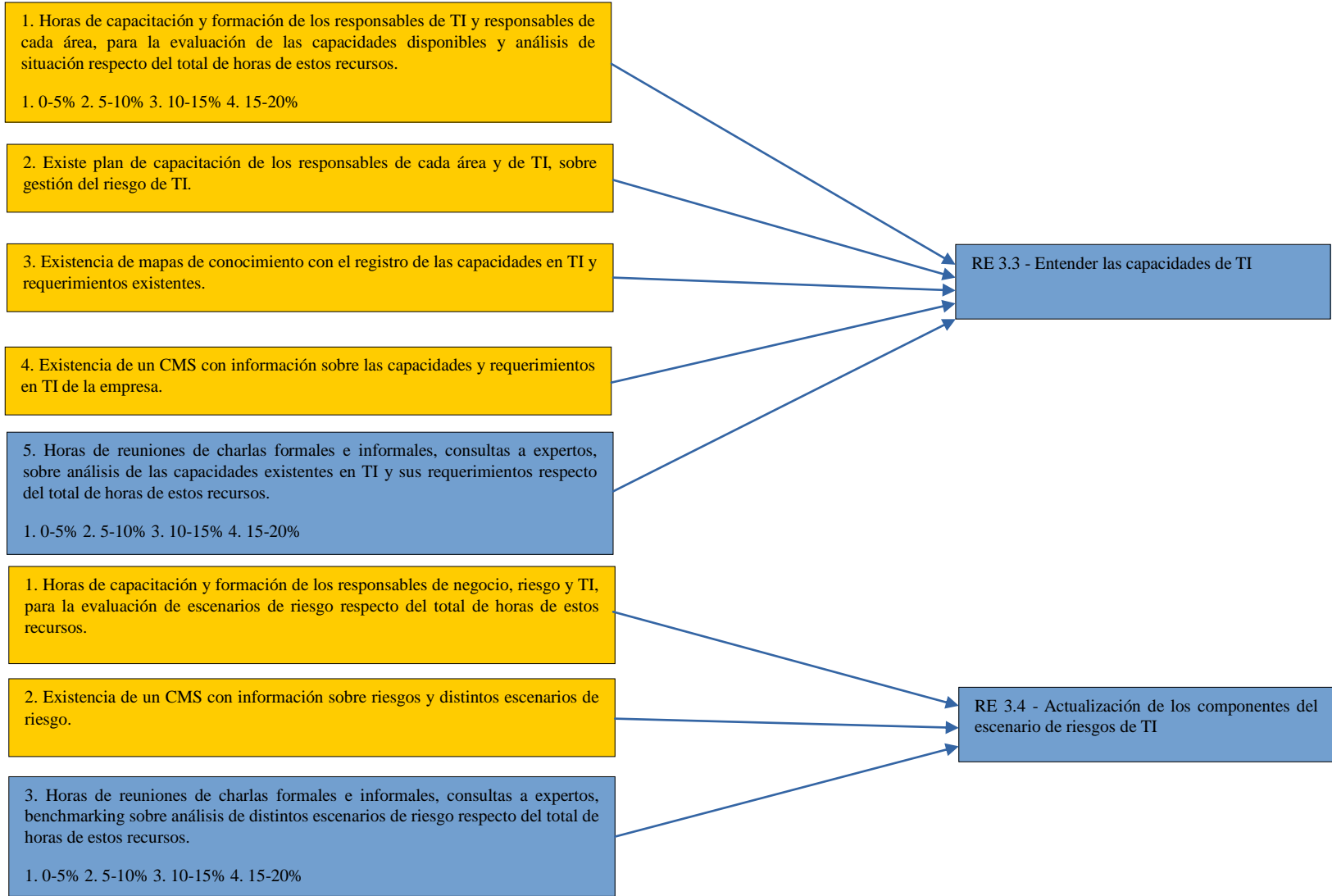


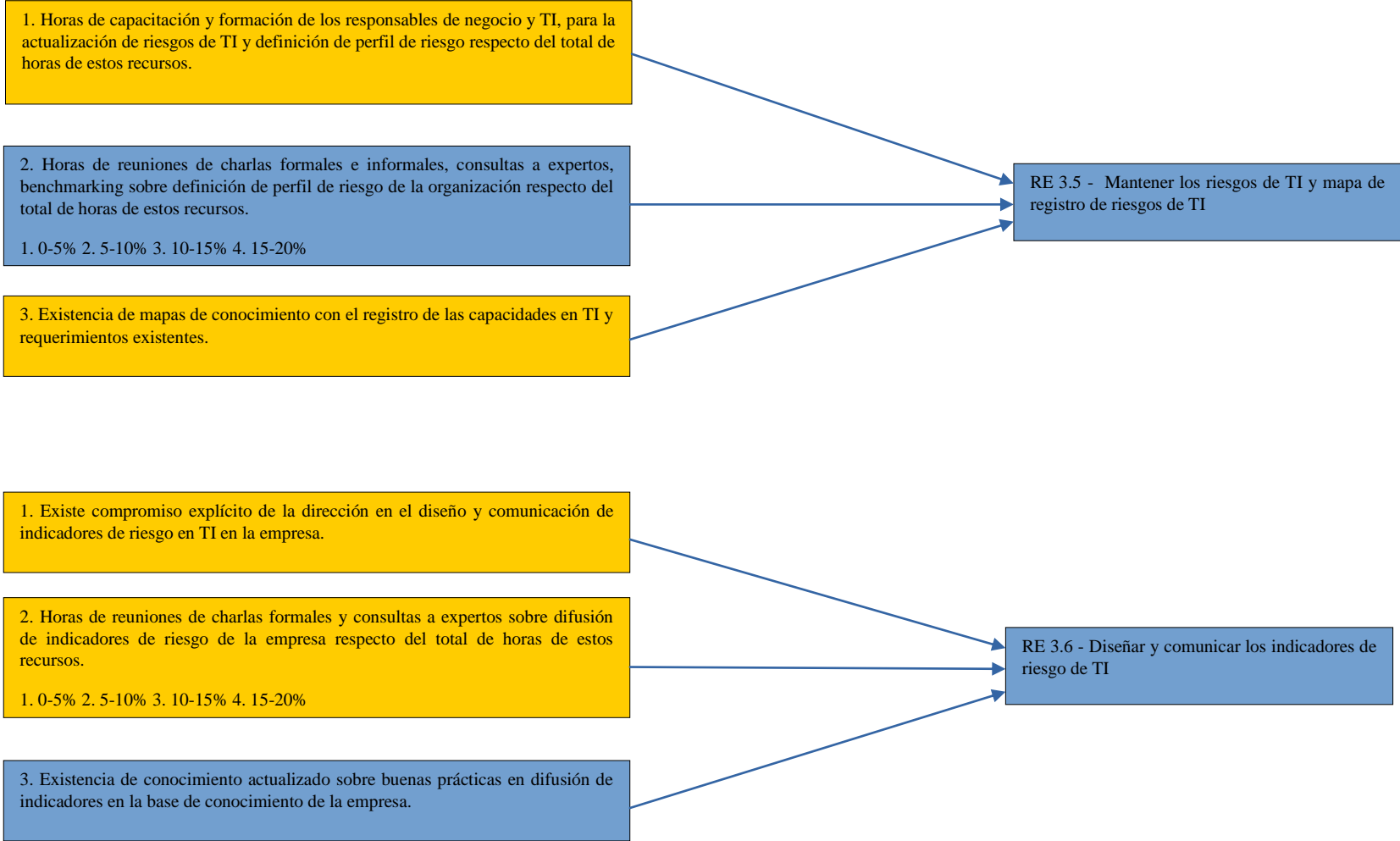


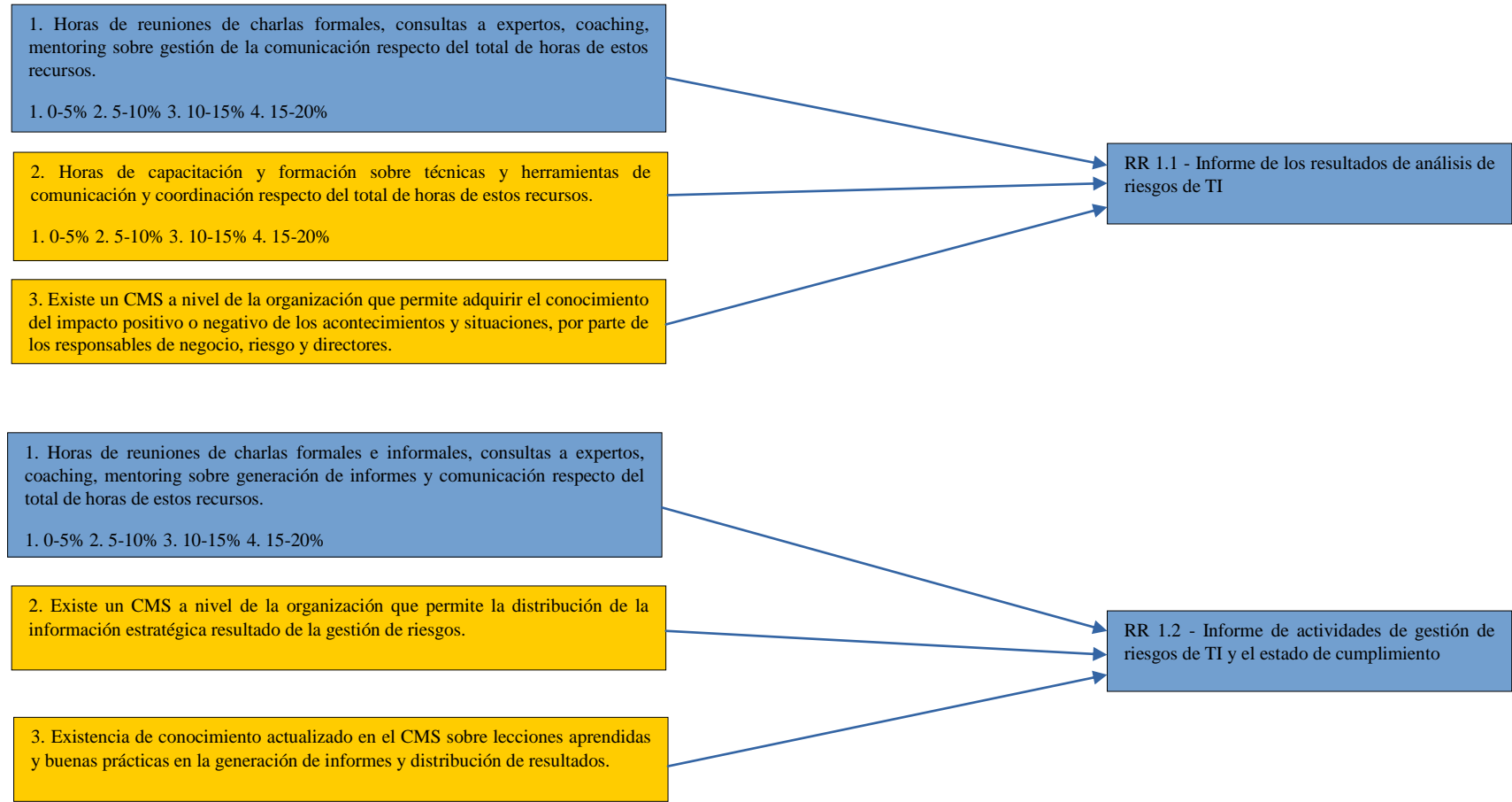


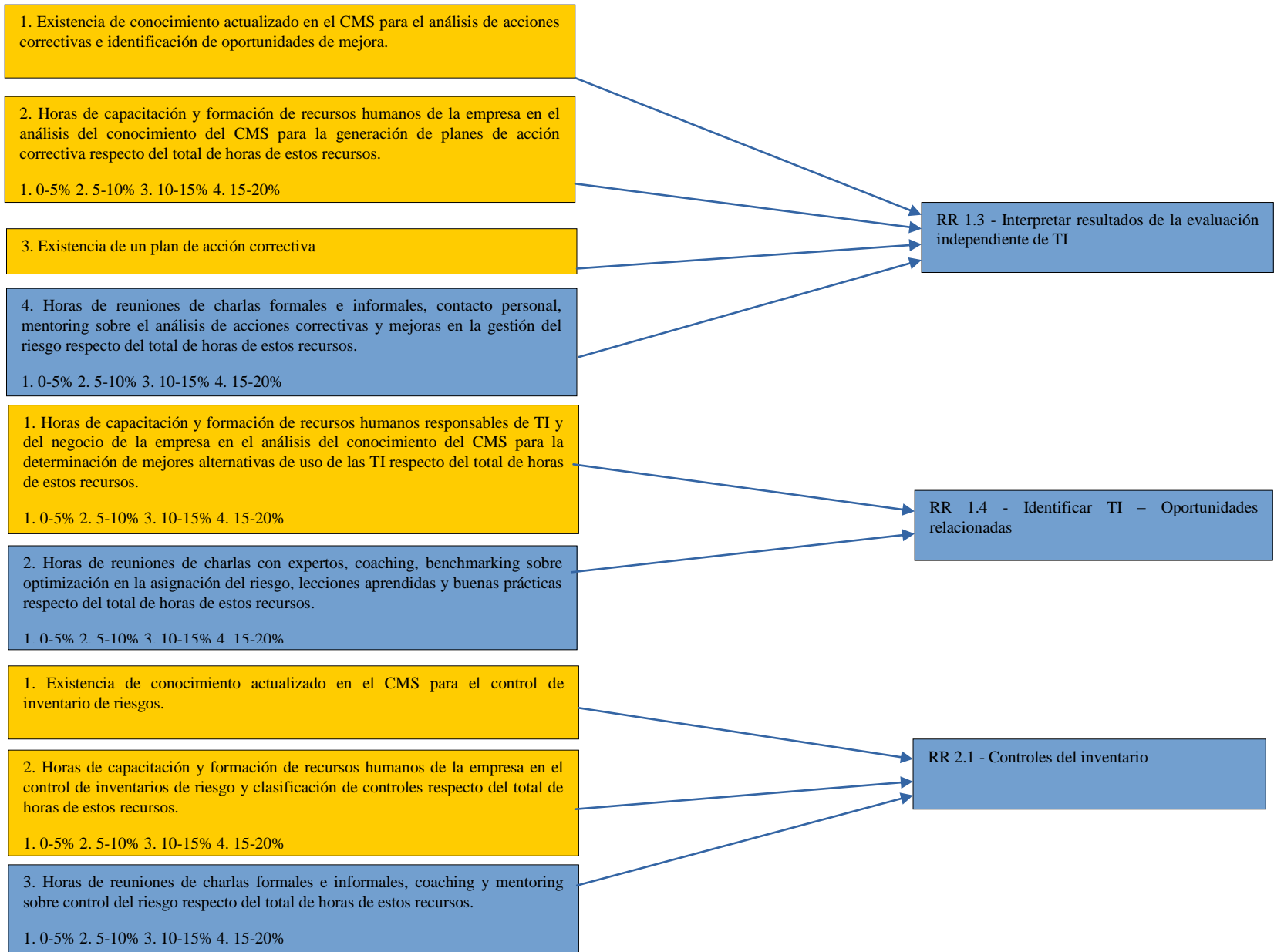


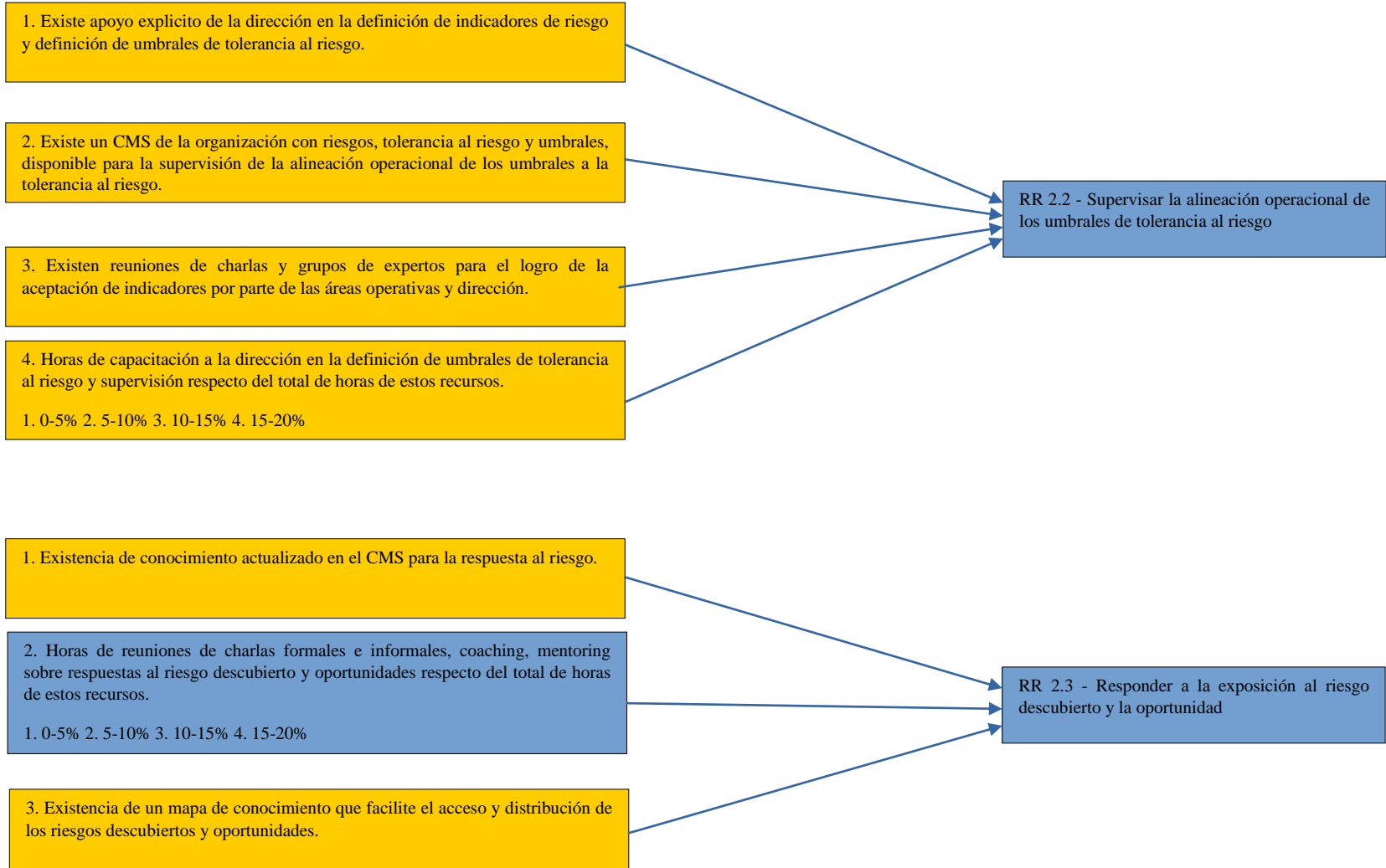


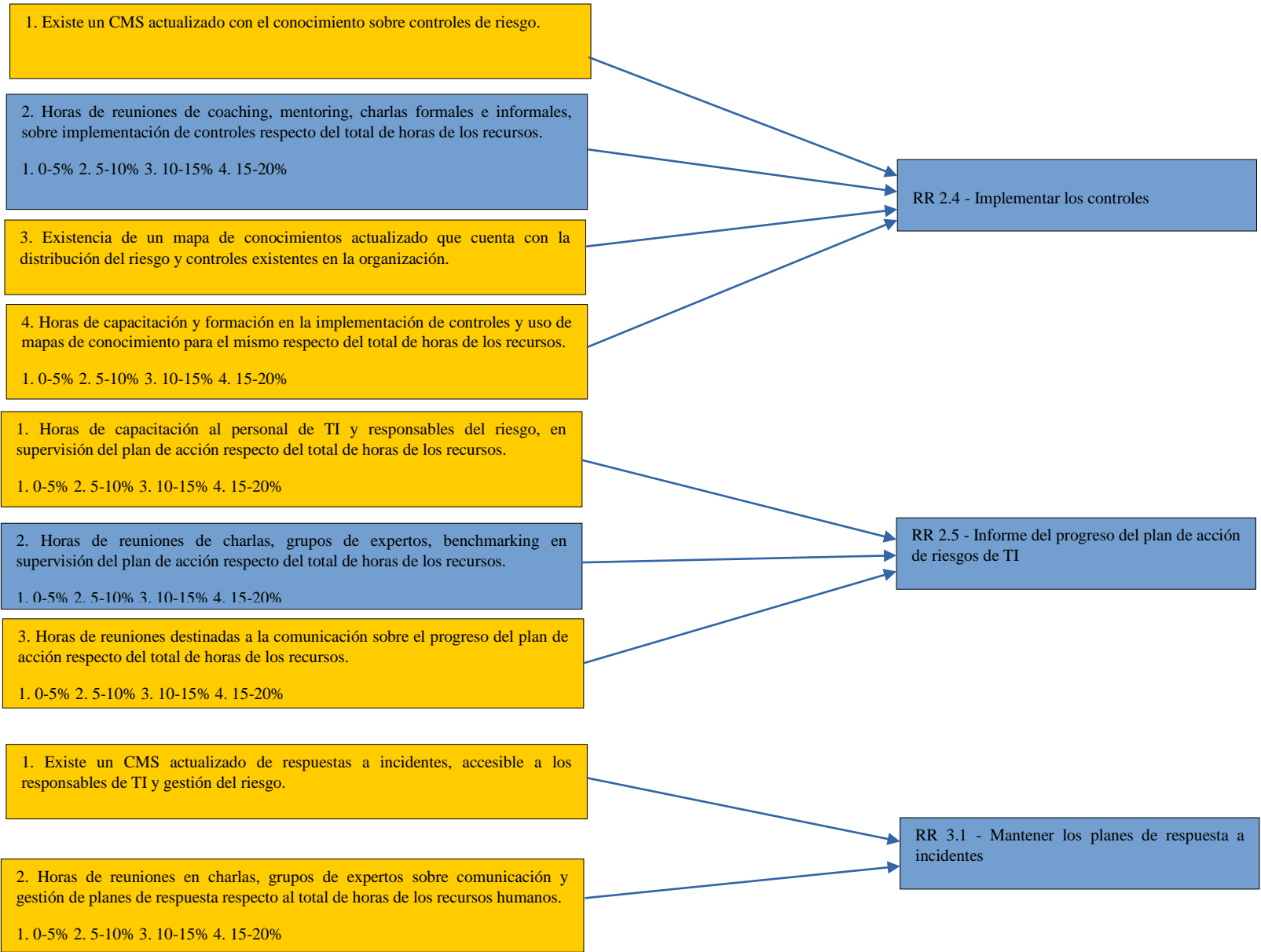


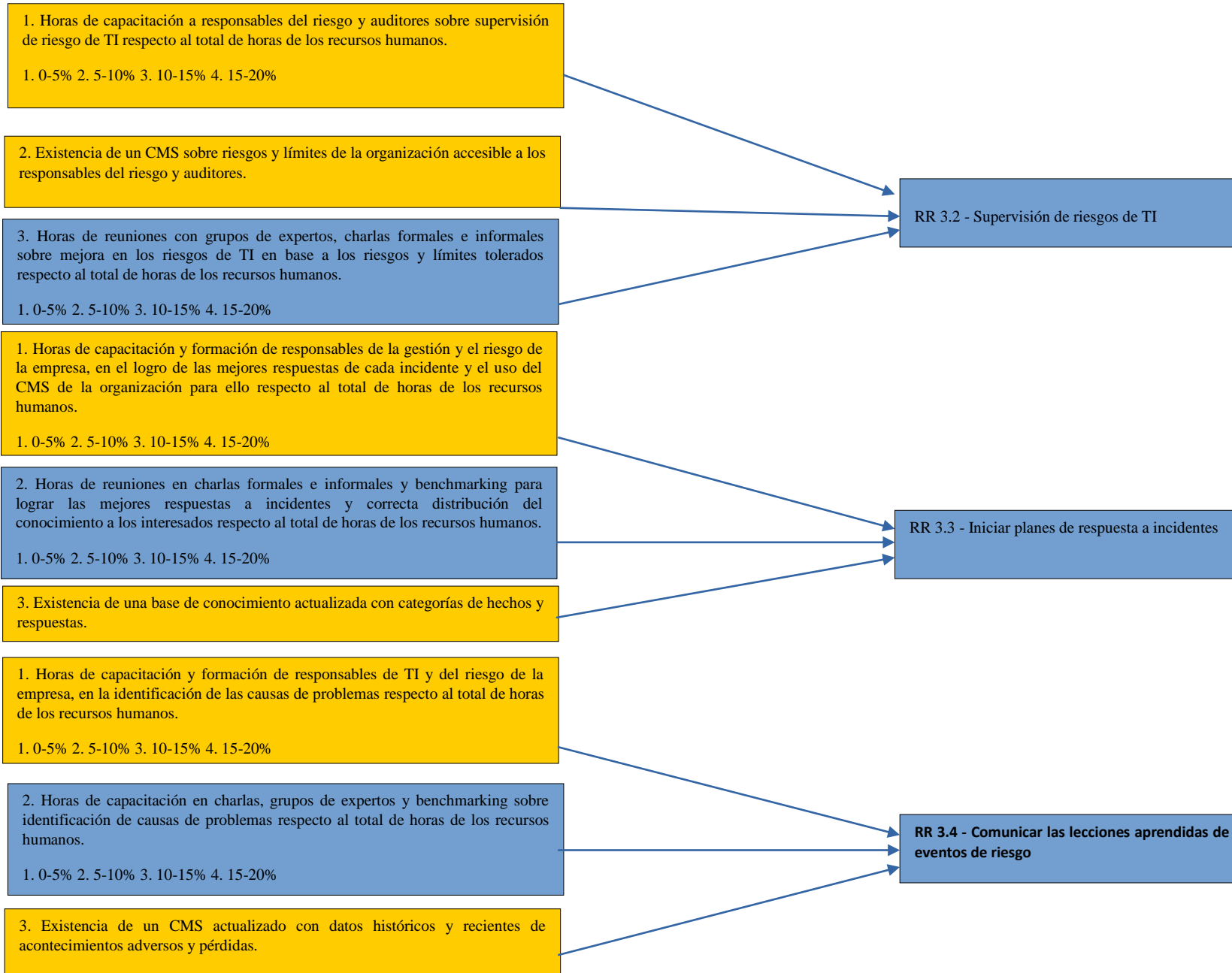












Anexo XVII – Justificación y ponderación de indicadores

Nivel 1 de madurez

	Proceso	Indicador	Medida
RG	Proceso Gobierno del Riesgo		
RG 1.1	Desarrollar en una empresa el marco específico de gestión de riesgos de TI	<p>1. Porcentaje de variables de negocio para las cuales se ha identificado y registrado los puntos de TI que pueden aportar valor al negocio, para los cuales existe un análisis de tolerancia al riesgo. Registro de variables con tolerancia al riesgo en los rangos: 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p> <p>2. Existencia de mapas de conocimiento que vinculan los eventos de TI identificados.</p>	<p>No existe una identificación y registro de variables de negocio y puntos de TI que pueden aportar valor al negocio con un análisis de tolerancia al riesgo. En algunos casos aislados solo se identifica alguna de estas variables.</p> <p>No existen mapas de conocimiento que vinculen los eventos de TI, o existe alguno en forma aislada para una tarea específica de un área aislada de la organización.</p>
RG 1.2	Proponer los umbrales de tolerancia de riesgos de TI	<p>1. Porcentaje de procesos de negocio que cuentan con medidas de riesgo y niveles de tolerancia asociados. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p> <p>2. Existencia de recursos humanos capacitados para la definición de umbrales de tolerancia de riesgos de TI. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>20% de los procesos de negocio identificados, cuenta con medidas de riesgo y nivel de tolerancia definido.</p> <p>20% de los recursos destinados a la definición de umbrales, cuenta con habilidades en la definición de umbrales de tolerancia sobre una base ad hoc, pero no son desarrollados activamente.</p>

RG 1.3	Aprobar la tolerancia al riesgo	1. Existencia de mapas de conocimiento y base de conocimiento de todas las áreas de la empresa con umbrales de riesgo por área de negocio.	No existen mapas de conocimiento y una base integrada de la organización con umbrales de riesgo, o existe algún mapa en forma aislada para una tarea específica de un área aislada de la organización.
RG 1.4	Alinear la política de riesgos de TI	1. Existencia de base de conocimiento de la organización con apetito al riesgo y tolerancia de cada área de negocio. 2. Nro. de horas de reunión de grupos de expertos por cada área sobre el número de áreas de negocio de la empresa, dedicados a la definición del apetito y tolerancia al riesgo de cada área respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No existe una base integrada de la organización con apetito al riesgo y tolerancia, o se registra en forma aislada para algunas áreas de la organización. El apetito y tolerancia al riesgo solo se consideran en evaluaciones de hechos ocurridos. 5% de las horas de los recursos humanos se destinan a la definición del apetito y tolerancia al riesgo.
RG 1.5	Promover los riesgos de TI – cultura consciente	1. Horas dedicadas en cursos sobre nro. de personas capacitadas en gestión del riesgo para cada área de negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% del total de horas se destina a cursos de capacitación en gestión del riesgo.
		2. Existencia de base de conocimientos con registro de acciones y buenas prácticas en gestión del riesgo de cada área de negocio. 3. Existencia del rol CKO dedicado a la comunicación de la política de gestión del riesgo en la organización.	No existe una base integrada de la organización con registro de acciones y buenas prácticas en gestión de riesgos, o se registra en forma aislada para algunas áreas de la organización. No aplica

		4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	No se reconoce la necesidad de administrar la exposición al riesgo, no existe conciencia del riesgo o es considerado un problema técnico, por lo que no se define una política de gestión del riesgo en la organización y por tanto no se realiza su promoción.
RG 1.6	Promover una comunicación efectiva de riesgos de TI	1. Existencia de un plan de comunicación de riesgos 2. Existencia de una base de conocimiento organizacional accesible por responsables y directores con información sobre amenazas e impacto de riesgos por área.	No aplica No existe una base de conocimiento con registro sobre amenazas e impacto de riesgos.
		3. Nro. de amenazas por área de negocio registradas en la base de conocimiento. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	20% de las amenazas identificadas son registradas.
RG 2.1	Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización. 1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes. 2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	No existe compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo a nivel de la organización. No aplica No aplica

<p>RG 2.2</p>	<p>Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial</p>	<p>1. Horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de reuniones dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de las horas de los recursos humanos se destinan a la definición de escalas, categorías y jerarquías de riesgos.</p> <p>La organización no reconoce la necesidad de administrar la exposición al riesgo del negocio y sus operaciones. 5% del total de horas se destina a reuniones de coordinación entre directores de TI y las distintas áreas.</p>
		<p>3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>No existe una definición clara y completa de las escalas, categorías y jerarquías de riesgos, ya que no existe una conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico.</p>
<p>RG 2.3</p>	<p>Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa</p>	<p>1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.</p> <p>2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.</p>	<p>No existe una base integrada de la organización con registro de prácticas en gestión de riesgos, o se registra en forma aislada para algunas áreas de la organización.</p> <p>No existen mapas de conocimiento de la organización con registro de buenas prácticas en gestión del riesgo, o existe algún mapa en forma aislada para una tarea específica de un área aislada de la organización.</p>

		<p>3. Porcentaje de recursos de la empresa capacitados o que asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>No más del 20% de los recursos de la empresa participa en la identificación de conocimiento para alinear las prácticas de TI con prácticas de riesgo, identificando eventos de TI y las condiciones que pueden afectar en el día a día, que en ocasiones se discuten en reuniones de gestión. No existe una identificación sistemática del conocimiento.</p>
RG 2.4	Proporcionar recursos adecuados para la gestión de riesgos	<p>1. Nro. de horas en capacitación al personal de cada área en gestión del riesgo, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de las horas de los recursos humanos se destinan a la capacitación en riesgos.</p>
		<p>2. Existencia de una base de conocimiento de la organización y mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	<p>No existen mapas de conocimiento y una base integrada de la organización con las relaciones de conocimiento existente en la empresa por rol y responsable, o existe algún mapa en forma aislada para una tarea específica de un área aislada de la organización.</p>
RG 2.5	Garantizar el aseguramiento independiente sobre la gestión de riesgos	<p>1. Existe una base de conocimiento con el registro del apetito al riesgo y tolerancia que permite la gestión del riesgo por parte del director de TI y director general.</p>	<p>No existe una base integrada de la organización con registro del apetito al riesgo y tolerancia que permita la gestión del riesgo, o se registra en forma aislada para algunas áreas de la organización.</p>

		<p>2. Existencia de mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	<p>No existen mapas de conocimiento de la organización con las relaciones de conocimiento existente por rol y responsable, o existe algún mapa en forma aislada para un área aislada de la organización.</p>
		<p>3. Horas en capacitación de recursos humanos asegurando su independencia en la gestión de riesgos respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Las habilidades de gestión de riesgos pueden existir sobre una base ad hoc pero no son desarrollados activamente.</p>
RG 3.1	Ganancia de la gestión de compra para el enfoque de análisis de riesgos	<p>1. Existe una base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo.</p>	<p>No existe una base integrada de la organización con registro de la calidad esperada en la toma de decisiones en gestión del riesgo, o se registra en forma aislada para algunas áreas de la organización.</p>
		<p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	<p>No existen mapas de conocimiento de la organización con las relaciones de conocimiento en riesgos de la empresa, o existe algún mapa en forma aislada para un área aislada de la organización.</p>
		<p>3. Horas de capacitación o reuniones que permitan interpretar los informes de análisis de riesgo y brechas existentes con el riesgo empresarial, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No hay una clara visión de futuro por lo cual la información sobre riesgos y su mitigación se deducen de lo ocurrido en el momento.</p>

		<p>4. Horas de capacitación en concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos de la empresa, respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico.</p>
RG 3.2	Aprobar el análisis de riesgos de TI	<p>1. Existe una base de conocimiento única para las distintas áreas de la empresa accesible a todos los directores de área que permite registrar, transmitir y usar dicho conocimiento.</p>	<p>No existe una base única de la organización que permita registrar, transmitir y usar el conocimiento en riesgos de la empresa, o existen bases en forma aislada para algunas áreas de la organización.</p>
		<p>2. Nro. de horas en capacitación y reuniones para la formación de los directores de área en la cultura de gestión del riesgo a través de la gestión del conocimiento respecto al total de horas de los directores.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% del total de horas de los directores se destina a reuniones o capacitación.</p>
RG 3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.</p>	<p>No existe una base de conocimiento de la organización que establezca la incidencia del riesgo en TI en el negocio, o existen bases en forma aislada para algunas áreas de la organización.</p>
		<p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	<p>No existen mapas de conocimiento de la organización con las relaciones de conocimiento en riesgos de la empresa, o existe algún mapa en forma aislada para un área aislada de la organización.</p>

		<p>3. Horas de capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de las horas de los recursos humanos se destinan a capacitación en gestión del riesgo de TI.</p>
RG 3.4	<p>Aceptar los riesgos de TI</p>	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.</p>	<p>No existe una base de conocimiento de la organización que establezca la incidencia del riesgo en TI en el negocio, o existen bases en forma aislada para algunas áreas de la organización.</p>
		<p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	<p>No existen mapas de conocimiento de la organización con las relaciones de conocimiento en riesgos de la empresa, o existe algún mapa en forma aislada para un área aislada de la organización.</p>
		<p>3. Horas de capacitación en formación al personal sobre aceptación y gestión del riesgo de TI para el negocio de cada área de la empresa respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de las horas de los recursos humanos se destinan a capacitación en aceptación y gestión del riesgo de TI.</p>

RG 3.5	Priorizar actividades de respuesta de riesgos de TI	1. Existe una base de conocimiento para la gestión del riesgo en la empresa disponible para el director general y director de TI, que permita registrar métricas para el seguimiento del cumplimiento de las actividades de TI, así como priorización de las mismas, con información sobre el apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles.	No existe una base de conocimiento de la organización que registre las métricas para el seguimiento del cumplimiento de actividades de TI, apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles, o existen bases en forma aislada para algunas áreas de la organización.
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	No existen mapas de conocimiento de la organización con las relaciones de conocimiento en riesgos de la empresa, o existe algún mapa en forma aislada para un área aislada de la organización.
		3. Horas de capacitación y formación al director general y de TI sobre seguimiento y planificación de riesgos en TI respecto al total de horas de los directores general y de TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de las horas del director general y de TI se destinan a capacitación y formación en seguimiento y planificación de riesgos en TI.
RE	Gestión del Riesgo Proceso Evaluación del Riesgo (RE)		
RE 1.1	Establecer y mantener un modelo para la recolección de datos	1. Existe apoyo explícito de la dirección para la concreción de la recopilación de datos para la formación de un repositorio único de conocimiento, así como en la culturización en gestión del conocimiento en la empresa.	La recopilación de datos es impulsada por evaluaciones ante un episodio determinado, así como el análisis de riesgos que puede existir sobre una base ad hoc y no se desarrolla activamente.

		2. Existe una estrategia de adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	No existe una estrategia de adquisición y retención del conocimiento en todas las áreas de la organización.
		3. Existe una implementación para la adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	No existe una implementación basada en una estrategia para la adquisición y retención del conocimiento en todas las áreas de la organización.
		4. Horas de capacitación y formación realizadas con el personal de la empresa respecto a la recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento en la organización, respecto al total de horas del personal. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	5% de las horas del personal se destinan a la capacitación y formación del personal respecto a la recopilación de datos para facilitar la toma de decisiones.
RE 1.2	Recopilar datos sobre el entorno externo	1. Horas de reuniones de benchmarking, charlas informales y con expertos, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Las reuniones realizadas en las distintas áreas de la empresa para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI, no superan el 5% de las horas dedicadas a esta actividad.
RE 1.3	Recopilar datos sobre eventos de riesgo	1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Las reuniones realizadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI en las distintas áreas de la empresa, no superan el 5% de las horas dedicadas a esta actividad.

RE 1.4	Identificar factores de riesgo	<p>1. Horas de reuniones de charlas con expertos, coaching, comunidades de práctica realizadas por directivos de TI y de las restantes áreas de la empresa, aplicadas para la identificación de riesgos, asociados a proyectos, programas, servicios existentes y futuros, etc. que pueden generar eventos de riesgo, respecto al total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de una base de conocimiento organizacional donde se integra información sobre proyectos, programas, servicios e incidentes.</p>	<p>5% de las horas de los recursos son aplicados a reuniones para la identificación de riesgos.</p> <p>No existe una base de conocimiento de la organización, que integre la información de proyectos, programas, servicios e incidentes.</p>
RE 2.1	Definir Alcance del Análisis de Riesgo	<p>1. Horas de capacitación y formación al personal responsable de la gestión del riesgo y del negocio de la empresa, en cuanto a gestión y evaluación del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Métodos de análisis son impulsados por evaluaciones ante un episodio determinado, así como el análisis de riesgos que puede existir sobre una base ad hoc y no se desarrolla activamente. 5% de horas destinadas a capacitación y formación en gestión y evaluación del riesgo.</p>
		<p>2. Horas de reuniones de charlas con expertos, benchmarking, realizadas con el personal responsable de la gestión del riesgo y el negocio sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Métodos de análisis son impulsados por evaluaciones ante un episodio determinado, así como el análisis de riesgos que puede existir sobre una base ad hoc y no se desarrolla activamente. 5% de horas destinadas a reuniones de charlas con expertos, benchmarking, sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo.</p>

RE 2.2	Estimación de riesgos en TI	<p>1. Horas de capacitación y formación a los responsables del riesgo y de negocio de la empresa, sobre análisis de información de riesgo (factores, frecuencia, magnitud y tolerancia al riesgo) para la estimación y definición de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Ante la no existencia de una base de conocimiento organizacional, los controles se basan en requisitos de cumplimiento que pueden variar ampliamente en relación al riesgo y operar en áreas aisladas. 5% de horas destinadas a capacitación y formación en estimación y definición de controles.</p>
		<p>2. Existencia de un CMS disponible para el análisis en la estimación de riesgos.</p>	<p>No existe una CMS que integre la información a nivel de la organización.</p>
		<p>3. Horas de reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Ante la no existencia de un CMS a nivel de la organización, la estimación de riesgos se optimiza y retroalimenta según la información disponible de las distintas áreas. 5% de horas destinadas a reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos.</p>
		<p>4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos en el CMS de la empresa.</p>	<p>No existe una CMS que integre la información a nivel de la organización. Las habilidades de gestión de riesgos pueden existir sobre una base ad hoc.</p>
RE 2.3	Identificar las opciones de respuesta de riesgo	<p>1. Horas de capacitación y formación a los directivos y responsables del riesgo sobre identificación de respuestas de riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Las respuestas de riesgo específicas no se consideran. 5% de horas destinadas a capacitación y formación en identificación de respuestas de riesgo.</p>

		2. Existencia de un CMS disponible para la consulta y actualización de respuestas de riesgo.	No existe una CMS que integre la información a nivel de la organización. Las respuestas de riesgo pueden existir sobre una base ad hoc.
		3. Horas de reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	La identificación de respuestas no se realiza de forma sistemática. 5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos.
		4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas de riesgos en el CMS de la empresa.	No existe una CMS que integre la información a nivel de la organización. La identificación de respuestas de riesgos pueden existir sobre una base ad hoc.
RE 2.4	Realizar una revisión por pares de los resultados de análisis de riesgos de TI	1. Horas de capacitación y formación a los responsables del riesgo sobre la aplicación de técnicas para el análisis de riesgos de TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Las respuestas de riesgo específicas no se consideran. 5% de horas destinadas a capacitación y formación en aplicación de técnicas para el análisis de riesgos de TI.
		2. Existencia de un CMS disponible para la actualización de la información sobre riesgos de TI en la empresa.	No existe una CMS que integre la información a nivel de la organización. La actualización de la información sobre riesgo puede existir sobre una base ad hoc.
		3. Horas de reuniones de charlas con expertos, charlas formales e informales, coaching en asignación de recursos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	El análisis de riesgos de TI no se realiza de forma sistemática. 5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, para la asignación de recursos.

		4. Aplicación de sistemas expertos en la resolución de la asignación de recursos.	Ocasionalmente se aplican herramientas de asignación de recursos.
RE 3.1	Mapa de recursos de TI para procesos de negocio	1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.	No existen mapas de conocimiento de la organización con las relaciones de riesgos y actividades de negocio en la empresa, o existe algún mapa en forma aislada para un área aislada de la organización.
		2. Horas de capacitación y formación a los responsables del riesgo en la empresa, sobre uso y análisis de mapas de conocimiento respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Solo existe una identificación ad hoc del conocimiento en riesgos. 5% de horas destinadas a capacitación y formación en el uso y análisis de mapas de conocimiento.
RE 3.2	Determinar la criticidad de los negocios de recursos de TI	1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.	No existen mapas de conocimiento de la organización con las relaciones de riesgos y actividades de negocio en la empresa, o existe algún mapa en forma aislada para un área aislada de la organización.
		2. Horas de capacitación y formación a los responsables de la gestión de los recursos en las distintas áreas de la empresa, sobre la determinación de criticidad de los recursos según los requerimientos de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Solo existe una identificación ad hoc del conocimiento en riesgos. 5% de horas destinadas a capacitación y formación en la determinación de criticidad de los recursos según los requerimientos de la organización.

		<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales para la definición de la criticidad de los recursos de TI en cada área respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>4. Existencia de un CMS con información sobre riesgos, recursos y su criticidad.</p>	<p>La evaluación de riesgos y las opciones de mitigación se deducen de la evaluación de los hechos. 5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, para la definición de la criticidad de los recursos de TI.</p> <p>No existe una CMS que integre la información de riesgos, recursos y su criticidad a nivel de la organización. La actualización de la información sobre riesgo puede existir sobre una base ad hoc.</p>
RE 3.3	Entender las capacidades de TI	<p>1. Horas de capacitación y formación de los responsables de TI y responsables de cada área, para la evaluación de las capacidades disponibles y análisis de situación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Las habilidades de gestión en la evaluación y análisis pueden existir sobre una base ad hoc. 5% de horas destinadas a capacitación y formación en la evaluación de capacidades disponibles y análisis de situación.</p>
		<p>2. Existe plan de capacitación de los responsables de cada área y de TI, sobre gestión del riesgo de TI.</p>	<p>La organización no reconoce la necesidad de administrar la exposición al riesgo o el reconocimiento está surgiendo pero se limita a evitar riesgos.</p>
		<p>3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.</p>	<p>No existen mapas de conocimiento de la organización con el registro de las capacidades de TI y requerimientos existentes, o existe algún mapa en forma aislada para un área aislada de la organización.</p>

		4. Existencia de un CMS con información sobre las capacidades y requerimientos en TI de la empresa.	No existe una CMS que integre la información de capacidades y requerimientos en TI a nivel de la organización. Puede existir sobre una base ad hoc.
		5. Horas de reuniones de charlas formales e informales, consultas a expertos, sobre análisis de las capacidades existentes en TI y sus requerimientos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Las capacidades y requerimientos de TI se deducen de la evaluación de los eventos de TI ocurridos. 5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, para el análisis de capacidades y requerimientos de TI existentes.
RE 3.4	Actualización de los componentes del escenario de riesgos de TI	1. Horas de capacitación y formación de los responsables de negocio, riesgo y TI, para la evaluación de escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Las habilidades de gestión en la evaluación y análisis pueden existir sobre una base ad hoc. 5% de horas destinadas a capacitación y formación en la evaluación de escenarios de riesgo.
		2. Existencia de un CMS con información sobre riesgos y distintos escenarios de riesgo.	No existe una CMS que integre la información de riesgos y distintos escenarios de riesgo a nivel de la organización. Puede existir sobre una base ad hoc.
		3. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre análisis de distintos escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Las capacidades y requerimientos de TI se deducen de la evaluación de los eventos de TI ocurridos. 5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, para el análisis de escenarios de riesgo.

RE 3.5	Mantener los riesgos de TI y mapa de registro de riesgos de TI	<p>1. Horas de capacitación y formación de los responsables de negocio y TI, para la actualización de riesgos de TI y definición de perfil de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre definición de perfil de riesgo de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.</p>	<p>La actualización de riesgos y definición de perfiles de riesgo pueden existir sobre una base ad hoc. 5% de horas destinadas a capacitación y formación en la actualización de riesgos y definición de perfiles.</p> <p>Los eventos de TI y las condiciones que pueden afectar el día a día en ocasiones se discuten en reuniones de gestión. 5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, para la definición de perfiles de riesgo.</p> <p>No existen mapas de conocimiento de la organización con el registro de las capacidades de TI y requerimientos existentes, o existe algún mapa en forma aislada para un área aislada de la organización.</p>
RE 3.6	Diseñar y comunicar los indicadores de riesgo de TI	<p>1. Existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo en TI en la empresa.</p>	<p>No existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo a nivel de la organización.</p>
		<p>2. Horas de reuniones de charlas formales y consultas a expertos sobre difusión de indicadores de riesgo de la empresa respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, para la difusión de indicadores.</p>

		3. Existencia de conocimiento actualizado sobre buenas prácticas en difusión de indicadores en la base de conocimiento de la empresa.	Se pueden aplicar algunas herramientas de gestión del conocimiento en la difusión de indicadores, pero no existe un marco de buenas prácticas definido.
RR	Gestión del Riesgo Proceso Respuesta del Riesgo (RR)		
RR 1.1	Informe de los resultados de análisis de riesgos de TI	1. Horas de reuniones de charlas formales, consultas a expertos, coaching, mentoring sobre gestión de la comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Los eventos de TI y las condiciones que pueden afectar el día a día en ocasiones se discuten en reuniones de gestión. 5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, destinados a la gestión de la comunicación.
		2. Horas de capacitación y formación sobre técnicas y herramientas de comunicación y coordinación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	La comunicación y coordinación respecto de los resultados del análisis de riesgos no existe o no está definida claramente. 5% de horas destinadas a capacitación y formación sobre técnicas y herramientas de comunicación y coordinación.
		3. Existe un CMS a nivel de la organización que permite adquirir el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, por parte de los responsables de negocio, riesgo y directores.	No existe una CMS que integre la información del impacto de los acontecimientos a nivel de la organización. Puede existir sobre una base ad hoc.

RR 1.2	Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	1. Horas de reuniones de charlas formales e informales, consultas a expertos, coaching, mentoring sobre generación de informes y comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Los eventos de TI y las condiciones que pueden afectar el día a día en ocasiones se discuten en reuniones de gestión. 5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, destinados a la generación de informes y comunicación.
		2. Existe un CMS a nivel de la organización que permite la distribución de la información estratégica resultado de la gestión de riesgos.	No existe una CMS que integre la información estratégica resultado de la gestión de riesgos. Puede existir sobre una base ad hoc.
		3. Existencia de conocimiento actualizado en el CMS sobre lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados.	Se pueden aplicar algunas herramientas de gestión del conocimiento sobre lecciones aprendidas y buenas prácticas en generación de informes, pero no existe un marco de buenas prácticas definido.
RR 1.3	Interpretar resultados de la evaluación independiente de TI	1. Existencia de conocimiento actualizado en el CMS para el análisis de acciones correctivas e identificación de oportunidades de mejora.	Se pueden aplicar algunas herramientas de gestión del conocimiento para el análisis de hechos puntuales ocurridos e identificación de mejoras que se discuten en reuniones de gestión, pero no existe una identificación sistemática de las oportunidades de mejora.
		2. Horas de capacitación y formación de recursos humanos de la empresa en el análisis del conocimiento del CMS para la generación de planes de acción correctiva respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No se cuenta con un CMS integrado a nivel de la organización. 5% de horas destinadas a capacitación y formación sobre análisis del conocimiento disponible para la generación de acciones correctivas.

		3. Existencia de un plan de acción correctiva	No aplica
		4. Horas de reuniones de charlas formales e informales, contacto personal, mentoring sobre el análisis de acciones correctivas y mejoras en la gestión del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Los eventos de TI y las condiciones que pueden afectar el día a día en ocasiones se discuten en reuniones de gestión. 5% de horas destinadas a reuniones de charlas con expertos, charlas formales e informales, destinados al análisis de acciones correctivas y mejoras en la gestión del riesgo.
RR 1.4	Identificar TI Oportunidades relacionadas	– 1. Horas de capacitación y formación de recursos humanos responsables de TI y del negocio de la empresa en el análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No aplica
		2. Horas de reuniones de charlas con expertos, coaching, benchmarking sobre optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	El factor tiempo y los recursos financieros inciden en la gestión del conocimiento, no existiendo una cultura organizacional de gestión del conocimiento, así como la aplicación de un marco de buenas prácticas
RR 2.1	Controles del inventario	1. Existencia de conocimiento actualizado en el CMS para el control de inventario de riesgos.	No existe. Solo existe una identificación ad hoc del conocimiento para cumplir con las actividades propias del negocio.

		<p>2. Horas de capacitación y formación de recursos humanos de la empresa en el control de inventarios de riesgo y clasificación de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>En ocasiones se utilizan algunas herramientas de gestión del conocimiento para la gestión del riesgo. 5% de horas de capacitación y formación, destinadas al control de inventarios en riesgo y clasificación de controles.</p>
		<p>3. Horas de reuniones de charlas formales e informales, coaching y mentoring sobre control del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>En ocasiones se utilizan algunas herramientas de gestión del conocimiento para la gestión del riesgo. 5% de horas de reuniones de charlas formales e informales, coaching y mentoring, destinadas al control del riesgo.</p>
RR 2.2	Supervisar la alineación operacional de los umbrales de tolerancia al riesgo	<p>1. Existe apoyo explícito de la dirección en la definición de indicadores de riesgo y definición de umbrales de tolerancia al riesgo.</p>	<p>Los eventos de TI y las condiciones que pueden afectar el día a día en las operaciones en ocasiones se discuten en reuniones de gestión, pero las respuestas de riesgo específicos no se consideran.</p>
		<p>2. Existe un CMS de la organización con riesgos, tolerancia al riesgo y umbrales, disponible para la supervisión de la alineación operacional de los umbrales a la tolerancia al riesgo.</p>	<p>Los inventarios ad hoc centrados en el control se encuentran dispersos en aplicaciones de escritorio.</p>
		<p>3. Existen reuniones de charlas y grupos de expertos para el logro de la aceptación de indicadores por parte de las áreas operativas y dirección.</p>	<p>Los controles sobre riesgos se basan en requisitos de cumplimiento y varían ampliamente según el riesgo. El conocimiento es generado en forma aislada.</p>

		<p>4. Horas de capacitación a la dirección en la definición de umbrales de tolerancia al riesgo y supervisión respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico.</p>
RR 2.3	<p>Responder a la exposición al riesgo descubierto y la oportunidad</p>	<p>1. Existencia de conocimiento actualizado en el CMS para la respuesta al riesgo.</p>	<p>No existe. Solo existe un registro ad hoc del conocimiento para cumplir con las actividades propias del negocio.</p>
		<p>2. Horas de reuniones de charlas formales e informales, coaching, mentoring sobre respuestas al riesgo descubierto y oportunidades respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>TI es considerado responsable de la evaluación de riesgos y las opciones de mitigación se deducen de la evaluación de los hechos ocurridos. 5% de las horas de reuniones y charlas, coaching y mentoring se pueden dedicar a la discusión de las respuestas de riesgo específicas.</p>
		<p>3. Existencia de un mapa de conocimiento que facilite el acceso y distribución de los riesgos descubiertos y oportunidades.</p>	<p>No existen mapas de conocimiento de la organización que faciliten el acceso y distribución de los riesgos descubiertos y oportunidades, o existe algún mapa en forma aislada para un área aislada de la organización.</p>
RR 2.4	<p>Implementar los controles</p>	<p>1. Existe un CMS actualizado con el conocimiento sobre controles de riesgo.</p>	<p>No existe. Solo existe un registro ad hoc del conocimiento para cumplir con las actividades propias del negocio.</p>
		<p>2. Horas de reuniones de coaching, mentoring, charlas formales e informales, sobre implementación de controles respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>5% de las horas de los recursos destinadas a reuniones sobre implementación de controles de riesgo.</p>

		3. Existencia de un mapa de conocimientos actualizado que cuenta con la distribución del riesgo y controles existentes en la organización.	No existen mapas de conocimiento de la organización que faciliten el acceso y distribución de los riesgos y controles existentes en la organización.
		4. Horas de capacitación y formación en la implementación de controles y uso de mapas de conocimiento para el mismo respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de las horas de los recursos destinadas a la implementación de controles y mapas de conocimiento.
RR 2.5	Informe del progreso del plan de acción de riesgos de TI	1. Horas de capacitación al personal de TI y responsables del riesgo, en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No aplica
		2. Horas de reuniones de charlas, grupos de expertos, benchmarking en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No aplica
		3. Horas de reuniones destinadas a la comunicación sobre el progreso del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	No aplica
RR 3.1	Mantener los planes de respuesta a incidentes	1. Existe un CMS actualizado de respuestas a incidentes, accesible a los responsables de TI y gestión del riesgo.	No existe un CMS con información sobre respuestas a incidentes a nivel de la organización. Puede existir sobre una base ad hoc.

		<p>2. Horas de reuniones en charlas, grupos de expertos sobre comunicación y gestión de planes de respuesta respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Los eventos de TI y las condiciones que pueden afectar el día a día en ocasiones se discuten en reuniones de gestión. 5% de horas destinadas a reuniones en charlas, grupos de expertos, destinados a la gestión de planes de respuesta y comunicación.</p>
RR 3.2	Supervisión de riesgos de TI	<p>1. Horas de capacitación a responsables del riesgo y auditores sobre supervisión de riesgo de TI respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de horas destinadas a capacitación y formación sobre supervisión del riesgo.</p>
		<p>2. Existencia de un CMS sobre riesgos y límites de la organización accesible a los responsables del riesgo y auditores.</p> <p>3. Horas de reuniones con grupos de expertos, charlas formales e informales sobre mejora en los riesgos de TI en base a los riesgos y límites tolerados respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe un CMS con información riesgos y límites a nivel de la organización. Puede existir sobre una base ad hoc.</p> <p>Los eventos de TI y las condiciones que pueden afectar el día a día en ocasiones se discuten en reuniones de gestión. 5% de horas destinadas a reuniones en charlas, grupos de expertos, destinados a la mejora en los riesgos de TI según los riesgos y límites tolerados.</p>
RR 3.3	Iniciar planes de respuesta a incidentes	<p>1. Horas de capacitación y formación de responsables de la gestión y el riesgo de la empresa, en el logro de las mejores respuestas de cada incidente y el uso del CMS de la organización para ello respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de horas destinadas a capacitación y formación sobre mejores respuestas a incidentes.</p>

		<p>2. Horas de reuniones en charlas formales e informales y benchmarking para lograr las mejores respuestas a incidentes y correcta distribución del conocimiento a los interesados respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Los eventos de TI y las condiciones que pueden afectar el día a día en ocasiones se discuten en reuniones de gestión. 5% de horas destinadas a reuniones en charlas, grupos de expertos, destinados a la mejora en la respuesta a riesgos de TI y su comunicación.</p>
		<p>3. Existencia de una base de conocimiento actualizada con categorías de hechos y respuestas.</p>	<p>No existe un CMS con información de categorías de hechos y respuestas a nivel de la organización. Puede existir sobre una base ad hoc.</p>
RR 3.4	Comunicar las lecciones aprendidas de eventos de riesgo	<p>1. Horas de capacitación y formación de responsables de TI y del riesgo de la empresa, en la identificación de las causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de horas destinadas a capacitación y formación sobre identificación de causas de problemas.</p>
		<p>2. Horas de capacitación en charlas, grupos de expertos y benchmarking sobre identificación de causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>No existe conciencia del riesgo o se tiene en cuenta pero es considerado un problema técnico. 5% de horas destinadas a reuniones y charlas con grupos de expertos y benchmarking sobre identificación de causas de problemas.</p>
		<p>3. Existencia de un CMS actualizado con datos históricos y recientes de acontecimientos adversos y pérdidas.</p>	<p>No existe un CMS con información histórica y reciente sobre acontecimientos adversos y pérdidas a nivel de la organización. Puede existir sobre una base ad hoc.</p>

Nivel 2 de madurez

	Proceso	Indicador	Medida
RG	Proceso Gobierno del Riesgo		
RG 1.1	Desarrollar en una empresa el marco específico de gestión de riesgos de TI	1. Porcentaje de variables de negocio para las cuales se ha identificado y registrado los puntos de TI que pueden aportar valor al negocio, para los cuales existe un análisis de tolerancia al riesgo. Registro de variables con tolerancia al riesgo en los rangos: 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	Se identifican y registran las variables de negocio y puntos de TI que pueden aportar valor al negocio con un análisis de tolerancia al riesgo en base a un inventario centralizado de riesgos de la organización, con el apoyo del CKO. Existe un registro de por lo menos el 40% de las variables identificadas y su tolerancia al riesgo.
		2. Existencia de mapas de conocimiento que vinculan los eventos de TI identificados.	Existen mapas de conocimiento que vinculan los eventos de TI, a nivel de la organización gestionados por el CKO.
RG 1.2	Proponer los umbrales de tolerancia de riesgos de TI	1. Porcentaje de procesos de negocio que cuentan con medidas de riesgo y niveles de tolerancia asociados. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	40% de los procesos de negocio identificados, cuenta con medidas de riesgo y nivel de tolerancia definido.
		2. Existencia de recursos humanos capacitados para la definición de umbrales de tolerancia de riesgos de TI. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	40% de los usuarios encargados de la definición de umbrales, capacitados en definición de umbrales de tolerancia. Se utilizan herramientas de gestión del conocimiento que facilitan la capacitación de los recursos humanos.
RG 1.3	Aprobar la tolerancia al riesgo	1. Existencia de mapas de conocimiento y base de conocimiento de todas las áreas de la empresa con umbrales de riesgo por área de negocio.	Existen mapas de conocimiento y base de conocimiento con umbrales de riesgo para cada área de negocio, a nivel de la organización gestionados por el CKO.

RG 1.4	Alinear la política de riesgos de TI	1. Existencia de base de conocimiento de la organización con apetito al riesgo y tolerancia de cada área de negocio.	Existe una base de conocimiento con apetito al riesgo y tolerancia para cada área de negocio, a nivel de la organización gestionada por el CKO.
		2. Nro. de horas de reunión de grupos de expertos por cada área sobre el número de áreas de negocio de la empresa, dedicados a la definición del apetito y tolerancia al riesgo de cada área respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existen procesos definidos, comunicados y estandarizados que establecen los niveles y umbrales, así como controles y responsabilidades. Se dedica 10% de horas en reuniones de grupos de expertos en la definición del apetito y tolerancia al riesgo.
RG 1.5	Promover los riesgos de TI – cultura consciente	1. Horas dedicadas en cursos sobre nro de personas capacitadas en gestión del riesgo para cada área de negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe una formación y sensibilización del personal en cuanto a riesgos y se maneja un lenguaje común para la comunicación de riesgos. Se dedica 10% de horas en capacitación en gestión del riesgo.
		2. Existencia de base de conocimientos con registro de acciones y buenas prácticas en gestión del riesgo de cada área de negocio.	Existe una base de conocimiento con el registro de acciones y buenas prácticas en gestión de riesgo a nivel de la organización, gestionada por el CKO.
		3. Existencia del rol CKO dedicado a la comunicación de la política de gestión del riesgo en la organización.	Existe una formación y sensibilización del personal en cuanto a riesgos y se maneja un lenguaje común para la comunicación de riesgos dirigida y gestionada por el CKO.

		4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	Existen políticas de respuesta a los riesgos que definen cuándo y cómo responder a estos. Se destina tiempo y recursos económicos en la capacitación de los RRHH, con el compromiso de la gerencia.
RG 1.6	Promover una comunicación efectiva de los riesgos de TI	1. Existencia de un plan de comunicación de riesgos	Existe una formación y sensibilización del personal en cuanto a riesgos y se maneja un lenguaje común para la comunicación de riesgos dirigida y gestionada por el CKO.
		2. Existencia de una base de conocimiento organizacional accesible por responsables y directores con información sobre amenazas e impacto de riesgos por área.	Existe una base de conocimiento de la organización sobre amenazas e impacto de riesgos por área, disponible para todos los responsables y directores.
		3. Nro. de amenazas por área de negocio registradas en la base de conocimiento. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	40% de las amenazas identificadas son registradas en la base de conocimiento de la organización.
RG 2.1	Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización. 1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes.	Existen políticas de respuesta a los riesgos que definen cuándo y cómo responder a estos. Se destina tiempo y recursos económicos en la capacitación de los RRHH, con el compromiso de la gerencia. Existe un plan de comunicación de riesgos de la organización el cual se desarrolla aplicando técnicas y herramientas de gestión del conocimiento.

		<p>2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>40% de los roles o responsabilidades definidas en la empresa, participan en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno.</p>
RG 2.2	<p>Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial</p>	<p>1. Horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se considera la gestión de riesgos como una cuestión empresarial capacitando y formando a los directores en el uso del conocimiento sobre riesgo. Se dedica 10% de horas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos.</p>
		<p>2. Horas de reuniones dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se considera la gestión de riesgos como una cuestión empresarial capacitando y formando a los directores en el uso del conocimiento sobre riesgo. Se dedica 10% de horas en reuniones de coordinación entre directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos.</p>
		<p>3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>Asiste al menos al 40% de las reuniones de definición de escalas, categorías y jerarquías de riesgos de la empresa, para su coordinación. La empresa considera la gestión de riesgos como una cuestión empresarial.</p>

RG 2.3	Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa	1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.	Existe una base de conocimiento de la organización sobre prácticas en gestión del riesgo, desarrollada en la organización por cada área y gestionada por el CKO.
		2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.	Existen mapas de conocimiento con registro de buenas prácticas en gestión del riesgo, a nivel de la organización, gestionados por el CKO.
RG 2.4	Proporcionar recursos adecuados para la gestión de riesgos	<p>3. Porcentaje de recursos de la empresa capacitados o que asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p> <p>1. Nro. de horas en capacitación al personal de cada área en gestión del riesgo, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de una base de conocimiento de la organización y mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	<p>40% de los recursos de la empresa son capacitados y/o asisten a reuniones sobre identificación y adquisición del conocimiento para alinear las prácticas de TI con las de gestión del riesgo.</p> <p>Se considera la gestión de riesgos como una cuestión empresarial capacitando y formando al personal en el uso del conocimiento sobre riesgo. Se dedica 10% de horas en capacitación sobre riesgos.</p> <p>Existen mapas de conocimiento y base de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable, a nivel de la organización, gestionados por el CKO.</p>

RG 2.5	Garantizar el aseguramiento independiente sobre la gestión de riesgos	<p>1. Existe una base de conocimiento con el registro del apetito al riesgo y tolerancia que permite la gestión del riesgo por parte del director de TI y director general.</p> <p>2. Existencia de mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	<p>Existe una base de conocimiento de la organización con registro del apetito al riesgo y tolerancia, disponible para el director de TI y director general, desarrollada en la organización por cada área y gestionada por el CKO.</p> <p>Existen mapas de conocimiento con registro de las relaciones de conocimiento existente por rol y responsable, a nivel de la organización, gestionados por el CKO.</p>
RG 3.1	Ganancia de la gestión de compra para el enfoque de análisis de riesgos	<p>3. Horas en capacitación de recursos humanos asegurando su independencia en la gestión de riesgos respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>1. Existe una base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo.</p>	<p>Existe una formación y sensibilización del personal en cuanto a riesgos, los usuarios son capacitados en amenazas relacionadas a TI, dedicando 10% de sus horas en capacitación sobre gestión del riesgo.</p> <p>Existe una base de conocimiento de la organización con registro de la calidad esperada en la toma de decisiones en gestión del riesgo, desarrollada en la organización por cada área y gestionada por el CKO.</p>
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Existen mapas de conocimiento con registro de las relaciones de conocimiento en riesgos, a nivel de la organización, gestionados por el CKO.

		<p>3. Horas de capacitación o reuniones que permitan interpretar los informes de análisis de riesgo y brechas existentes con el riesgo empresarial, respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se dedica 10% de horas en formación del personal en cuanto a interpretación de informes de análisis de riesgo y brechas con el riesgo empresarial.</p>
		<p>4. Horas de capacitación en concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos de la empresa, respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se dedica 10% de horas en capacitación sobre formación y sensibilización del personal en cuanto a la comprensión sobre la importancia de los riesgos de TI en la gestión de riesgos de la empresa.</p>
RG 3.2	Aprobar el análisis de riesgos de TI	<p>1. Existe una base de conocimiento única para las distintas áreas de la empresa accesible a todos los directores de área que permite registrar, transmitir y usar dicho conocimiento.</p>	<p>Existe una base de conocimiento de la organización que se desarrolla en cada área y es gestionada por el CKO.</p>
		<p>2. Nro. de horas en capacitación y reuniones para la formación de los directores de área en la cultura de gestión del riesgo a través de la gestión del conocimiento respecto al total de horas de los directores.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se dedica 10% de horas en capacitación y reuniones para la formación de los directores en la cultura de gestión del riesgo.</p>
RG 3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.</p>	<p>Existe una base de conocimiento de la organización que establece la incidencia del riesgo en TI en el negocio, que se desarrolla en cada área y es gestionada por el CKO.</p>

		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Existen mapas de conocimiento con registro de las relaciones del conocimiento en riesgos, a nivel de la organización, gestionados por el CKO.
		3. Horas de capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se dedica 10% de horas en capacitación del personal en cuanto a concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio.
RG 3.4	Aceptar los riesgos de TI	1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa. 2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Existe una base de conocimiento de la organización que establece la incidencia del riesgo en TI en el negocio, que se desarrolla en cada área y es gestionada por el CKO. Existen mapas de conocimiento con registro de las relaciones del conocimiento en riesgos, a nivel de la organización, gestionados por el CKO.
		3. Horas de capacitación en formación al personal sobre aceptación y gestión del riesgo de TI para el negocio de cada área de la empresa respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se dedica 10% de horas en capacitación del personal en cuanto a aceptación y gestión del riesgo de TI para el negocio.

RG 3.5	Priorizar actividades de respuesta de riesgos de TI	1. Existe una base de conocimiento para la gestión del riesgo en la empresa disponible para el director general y director de TI, que permita registrar métricas para el seguimiento del cumplimiento de las actividades de TI, así como priorización de las mismas, con información sobre el apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles.	Existe una base de conocimiento de la organización donde se registran las métricas para el seguimiento del cumplimiento de actividades de TI, apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles, que se desarrolla en cada área y es gestionada por el CKO.
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa. 3. Horas de capacitación y formación al director general y de TI sobre seguimiento y planificación de riesgos en TI respecto al total de horas de los directores general y de TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existen mapas de conocimiento con registro de las relaciones del conocimiento en riesgos, a nivel de la organización, gestionados por el CKO. Se dedica 10% de horas en capacitación del director general y de TI en cuanto a seguimiento y planificación de riesgos en TI.
RE	Gestión del Riesgo Proceso Evaluación del Riesgo (RE)		
RE 1.1	Establecer y mantener un modelo para la recolección de datos	1. Existe apoyo explícito de la dirección para la concreción de la recopilación de datos para la formación de un repositorio único de conocimiento, así como en la culturización en gestión del conocimiento en la empresa.	Existe una formación del personal en cuanto a riesgos, se considera la gestión de riesgos como una cuestión empresarial, capacitando y formando en el uso del conocimiento sobre riesgo.
		2. Existe una estrategia de adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	Existe una estrategia de adquisición y retención del conocimiento para la gestión del riesgo.

		3. Existe una implementación para la adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	Se adquiere y retiene el conocimiento según la estrategia definida para la gestión del riesgo.
		4. Horas de capacitación y formación realizadas con el personal de la empresa respecto a la recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento en la organización, respecto al total de horas del personal. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se dedica 10% de horas en capacitación del personal en cuanto a recopilación de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento.
RE 1.2	Recopilar datos sobre el entorno externo	1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.	Se dedica 10% de horas en reuniones aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.
RE 1.3	Recopilar datos sobre eventos de riesgo	1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se dedica 10% de horas en reuniones aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.

RE 1.4	Identificar factores de riesgo	<p>1. Horas de reuniones de charlas con expertos, coaching, comunidades de práctica realizadas por directivos de TI y de las restantes áreas de la empresa, aplicadas para la identificación de riesgos, asociados a proyectos, programas, servicios existentes y futuros, etc. que pueden generar eventos de riesgo, respecto al total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de una base de conocimiento organizacional donde se integra información sobre proyectos, programas, servicios e incidentes.</p>	<p>10% de las horas de los recursos son aplicados a reuniones para la identificación de riesgos.</p> <p>Existe una base de conocimiento de la organización donde se integra información sobre proyectos, programas, servicios e incidentes, que se desarrolla en cada área y es gestionada por el CKO.</p>
RE 2.1	Definir Alcance del Análisis de Riesgo	<p>1. Horas de capacitación y formación al personal responsable de la gestión del riesgo y del negocio de la empresa, en cuanto a gestión y evaluación del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Existe una formación del personal en cuanto a riesgos, se considera la gestión de riesgos como una cuestión empresarial, capacitando y formando en el uso del conocimiento sobre gestión y evaluación del riesgo. 10% de las horas dedicadas a la capacitación y formación en gestión y evaluación del riesgo.</p>

		<p>2. Horas de reuniones de charlas con expertos, benchmarking, realizadas con el personal responsable de la gestión del riesgo y el negocio sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Existe una formación del personal en cuanto a riesgos, se considera la gestión de riesgos como una cuestión empresarial, capacitando y formando en el uso del conocimiento sobre gestión y evaluación del riesgo. 10% de las horas dedicadas a la capacitación y formación en gestión y evaluación del riesgo.</p>
RE 2.2	Estimación de riesgos en TI	<p>1. Horas de capacitación y formación a los responsables del riesgo y de negocio de la empresa, sobre análisis de información de riesgo (factores, frecuencia, magnitud y tolerancia al riesgo) para la estimación y definición de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de un CMS disponible para el análisis en la estimación de riesgos.</p>	<p>Los usuarios son capacitados en análisis de información de riesgo para estimación y definición de controles con la aplicación de técnicas de gestión del conocimiento. 10% de horas destinadas a capacitación y formación en estimación y definición de controles.</p> <p>Existe un CMS de la organización donde se registran las métricas para el seguimiento del cumplimiento de actividades de TI, apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles, que se desarrolla en cada área y es gestionada por el CKO.</p>
		<p>3. Horas de reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Charlas con expertos para optimización y retroalimentación de la información del CMS para la estimación de riesgos, son gestionados y facilitados por el CKO. 10% de horas destinadas a capacitación y formación en estimación y definición de controles.</p>

		4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos en el CMS de la empresa.	Existe un CMS de la organización con información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos, que se desarrolla en cada área y es gestionada por el CKO.
RE 2.3	Identificar las opciones de respuesta de riesgo	1. Horas de capacitación y formación a los directivos y responsables del riesgo sobre identificación de respuestas de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Los directivos y responsables del riesgo son capacitados en identificación de respuestas de riesgo con la aplicación de técnicas de gestión del conocimiento. 10% de horas destinadas a capacitación y formación en identificación de respuestas al riesgo.
		2. Existencia de un CMS disponible para la consulta y actualización de respuestas de riesgo. 3. Horas de reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe un CMS de la organización donde se registran las respuestas al riesgo, se desarrolla en cada área y es gestionada por el CKO. Charlas con expertos, charlas formales e informales para optimización y retroalimentación de la información del CMS para la identificación de respuestas al riesgo, son gestionados y facilitados por el CKO. 10% de horas destinadas a capacitación y formación en identificación de respuestas al riesgo.
		4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas de riesgos en el CMS de la empresa.	Existe un CMS de la organización con información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas al riesgo, que se desarrolla en cada área y es gestionada por el CKO.

RE 2.4	Realizar una revisión por pares de los resultados de análisis de riesgos de TI	<p>1. Horas de capacitación y formación a los responsables del riesgo sobre la aplicación de técnicas para el análisis de riesgos de TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de un CMS disponible para la actualización de la información sobre riesgos de TI en la empresa.</p>	<p>Los responsables del riesgo son capacitados en la aplicación de técnicas para el análisis de riesgos de TI. 10% de horas destinadas a capacitación y formación en la aplicación de técnicas de análisis de riesgos de TI.</p> <p>Existe un CMS de la organización donde se registran los resultados de análisis de riesgos de TI, se desarrolla en cada área y es gestionada por el CKO.</p>
		<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales, coaching en asignación de recursos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Charlas con expertos, charlas formales e informales para optimización y retroalimentación de la información del CMS para la asignación de recursos, son gestionados y facilitados por el CKO. 10% de horas destinadas a capacitación y formación en asignación de recursos.</p>
		<p>4. Aplicación de sistemas expertos en la resolución de la asignación de recursos.</p>	<p>Se aplican sistemas expertos en la resolución de la asignación de recursos.</p>
RE 3.1	Mapa de recursos de TI para procesos de negocio	<p>1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.</p> <p>3. Horas de capacitación y formación a los responsables del riesgo en la empresa, sobre uso y análisis de mapas de conocimiento respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Existen mapas de conocimiento con registro de las relaciones entre riesgos y actividades de negocio, a nivel de la organización, gestionados por el CKO.</p> <p>Se dedica 10% de horas en capacitación y formación a los responsables de la empresa en cuanto al uso y análisis de mapas de conocimiento.</p>

RE 3.2	Determinar la criticidad de los negocios de recursos de TI	1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.	Existen mapas de conocimiento con registro de las relaciones entre riesgos y actividades de negocio, a nivel de la organización, gestionados por el CKO.
		<p>2. Horas de capacitación y formación a los responsables de la gestión de los recursos en las distintas áreas de la empresa, sobre la determinación de criticidad de los recursos según los requerimientos de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Horas de reuniones de charlas con expertos, charlas formales e informales para la definición de la criticidad de los recursos de TI en cada área respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se dedica 10% de horas en capacitación y formación a los responsables de la gestión de los recursos en cuanto a la determinación de la criticidad de los recursos según los requerimientos de la organización.</p> <p>Charlas con expertos, charlas formales e informales para optimización y retroalimentación de la información del CMS en cuanto a la definición de la criticidad de los recursos de TI, son gestionados y facilitados por el CKO. 10% de horas destinadas a capacitación y formación en definición de la criticidad de los recursos de TI.</p>
		4. Existencia de un CMS con información sobre riesgos, recursos y su criticidad.	Existe un CMS de la organización donde se registra la información sobre riesgos, recursos y su criticidad, se desarrolla en cada área y es gestionada por el CKO.

RE 3.3	Entender las capacidades de TI	<p>1. Horas de capacitación y formación de los responsables de TI y responsables de cada área, para la evaluación de las capacidades disponibles y análisis de situación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se dedica 10% de horas en capacitación y formación a los responsables de TI y de cada área, en cuanto a la evaluación de capacidades y análisis de situación según los requerimientos de la organización.</p>
		<p>2. Existe plan de capacitación de los responsables de cada área y de TI, sobre gestión del riesgo de TI.</p>	<p>Existe un plan de capacitación sobre gestión de riesgo de TI, gestionado por CKO.</p>
		<p>3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.</p>	<p>Existen mapas de conocimiento con registro de las capacidades y requerimientos de TI existentes, a nivel de la organización, gestionados por el CKO.</p>
		<p>4. Existencia de un CMS con información sobre las capacidades y requerimientos en TI de la empresa.</p>	<p>Existe un CMS de la organización donde se registra la información sobre capacidades y requerimientos de TI que se desarrolla en cada área y es gestionada por el CKO.</p>
		<p>5. Horas de reuniones de charlas formales e informales, consultas a expertos, sobre análisis de las capacidades existentes en TI y sus requerimientos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Charlas con expertos, charlas formales e informales para optimización y retroalimentación del CMS en cuanto al análisis de las capacidades y requerimientos de TI, son gestionados y facilitados por el CKO. 10% de horas destinadas a capacitación y formación en análisis de capacidades y requerimientos de TI.</p>

RE 3.4	Actualización de los componentes del escenario de riesgos de TI	<p>1. Horas de capacitación y formación de los responsables de negocio, riesgo y TI, para la evaluación de escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de un CMS con información sobre riesgos y distintos escenarios de riesgo.</p>	<p>Se dedica 10% de horas en capacitación y formación a los responsables de negocio, riesgo y TI, en cuanto a la evaluación de escenarios de riesgo.</p> <p>Existe un CMS de la organización donde se registra la información sobre riesgos y distintos escenarios de riesgo, que se desarrolla en cada área y es gestionada por el CKO.</p>
		<p>3. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre análisis de distintos escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Charlas con expertos, charlas formales e informales para optimización y retroalimentación del CMS en cuanto al análisis de distintos escenarios de riesgo, son gestionados y facilitados por el CKO. 10% de horas destinadas a capacitación y formación en análisis de escenarios de riesgo.</p>
RE 3.5	Mantener los riesgos de TI y mapa de registro de riesgos de TI	<p>1. Horas de capacitación y formación de los responsables de negocio y TI, para la actualización de riesgos de TI y definición de perfil de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se dedica 10% de horas en capacitación y formación a los responsables de negocio y TI, en cuanto a la actualización de riesgos y definición de perfiles de riesgo.</p>

		<p>2. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre definición de perfil de riesgo de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Charlas con expertos, charlas formales e informales para optimización y retroalimentación del CMS en cuanto a definición de perfiles de riesgo, son gestionados y facilitados por el CKO. 10% de horas destinadas a capacitación y formación en definición de perfiles de riesgo.</p>
		<p>3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.</p>	<p>Existen mapas de conocimiento con registro de las capacidades en TI y requerimientos existentes, a nivel de la organización, gestionados por el CKO.</p>
RE 3.6	Diseñar y comunicar los indicadores de riesgo de TI	<p>1. Existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo en TI en la empresa.</p>	<p>Existen políticas que definen la comunicación de indicadores de riesgos en TI en la empresa. Se destina tiempo y recursos económicos en la capacitación de los RRHH, con el compromiso de la gerencia.</p>
		<p>2. Horas de reuniones de charlas formales y consultas a expertos sobre difusión de indicadores de riesgo de la empresa respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se realizan charlas con expertos, charlas formales e informales para optimizar la difusión de indicadores, las que son gestionadas y facilitadas por el CKO. 10% de horas destinadas a capacitación y formación en difusión de indicadores.</p>
RR	Gestión del Riesgo Proceso Respuesta del Riesgo (RR)	<p>3. Existencia de conocimiento actualizado sobre buenas prácticas en difusión de indicadores en la base de conocimiento de la empresa.</p>	<p>Se registra la información sobre buenas prácticas en difusión de indicadores en la base de conocimiento, que se desarrolla en cada área y es gestionada por el CKO.</p>

RR 1.1	Informe de los resultados de análisis de riesgos de TI	<p>1. Horas de reuniones de charlas formales, consultas a expertos, coaching, mentoring sobre gestión de la comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de capacitación y formación sobre técnicas y herramientas de comunicación y coordinación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican técnicas de gestión del conocimiento para optimizar la gestión de la comunicación, las que son gestionadas y facilitadas por el CKO. 10% de horas destinadas a capacitación y formación en gestión de la comunicación.</p> <p>Se dedica 10% de horas en capacitación y formación sobre técnicas y herramientas de comunicación y coordinación.</p>
		3. Existe un CMS a nivel de la organización que permite adquirir el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, por parte de los responsables de negocio, riesgo y directores.	Existe un CMS de la organización donde se registra la información sobre el impacto de los acontecimientos y situaciones de riesgo, que se desarrolla en cada área y es gestionada por el CKO.
RR 1.2	Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	<p>1. Horas de reuniones de charlas formales e informales, consultas a expertos, coaching, mentoring sobre generación de informes y comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican técnicas de gestión del conocimiento para optimizar la generación de informes y su comunicación, que son gestionadas y facilitadas por el CKO. 10% de horas destinadas a capacitación y formación en generación de informes y su comunicación.</p>
		2. Existe un CMS a nivel de la organización que permite la distribución de la información estratégica resultado de la gestión de riesgos.	Existe un CMS de la organización donde se registra la información estratégica en gestión de riesgos, que se desarrolla en cada área y es gestionada por el CKO.

		3. Existencia de conocimiento actualizado en el CMS sobre lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados.	Se registra la información sobre buenas prácticas y lecciones aprendidas en generación y distribución de informes en la base de conocimiento, que se desarrolla en cada área y es gestionada por el CKO.
RR 1.3	Interpretar resultados de la evaluación independiente de TI	1. Existencia de conocimiento actualizado en el CMS para el análisis de acciones correctivas e identificación de oportunidades de mejora.	Las acciones correctivas e identificación de oportunidades de mejora se registran en la base de conocimiento, que se desarrolla en cada área y es gestionada por el CKO.
		2. Horas de capacitación y formación de recursos humanos de la empresa en el análisis del conocimiento del CMS para la generación de planes de acción correctiva respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se dedica 10% de horas en capacitación y formación sobre análisis del conocimiento del CMS para la generación de planes de acción correctiva.
		3. Existencia de un plan de acción correctiva 4. Horas de reuniones de charlas formales e informales, contacto personal, mentoring sobre el análisis de acciones correctivas y mejoras en la gestión del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe un plan de acción correctiva de la organización el cual se desarrolla aplicando técnicas y herramientas de gestión del conocimiento. Se aplican técnicas de gestión del conocimiento para optimizar el análisis de acciones correctivas y mejoras en la gestión del riesgo, que son gestionadas y facilitadas por el CKO. 10% de horas destinadas a capacitación y formación en análisis de acciones correctivas y mejoras en la gestión del riesgo.

RR 1.4	Identificar TI Oportunidades relacionadas	–	1. Horas de capacitación y formación de recursos humanos responsables de TI y del negocio de la empresa en el análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se considera la gestión de riesgos como una cuestión empresarial capacitando y formando a los responsables de TI y del negocio en el uso del conocimiento para la determinación de mejores alternativas de uso de las TI. 10% de horas destinadas a capacitación y formación en análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI.
			2. Horas de reuniones de charlas con expertos, coaching, benchmarking sobre optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Actividades de gestión del riesgo alineadas en toda la empresa, aplicando herramientas de gestión del conocimiento como lecciones aprendidas y grupos de expertos. 10% de horas destinadas a reuniones de charlas con expertos, coaching, benchmarking para la optimización en la asignación del riesgo.
RR 2.1	Controles inventario	del	1. Existencia de conocimiento actualizado en el CMS para el control de inventario de riesgos.	Se define un inventario centralizado de los problemas de riesgo, definiendo una base de conocimiento común a toda la organización.
			2. Horas de capacitación y formación de recursos humanos de la empresa en el control de inventarios de riesgo y clasificación de controles respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se destina tiempo y recursos económicos en la capacitación de los recursos humanos, que permite el adecuado control de inventarios y clasificación de controles de riesgo. 10% de las horas de capacitación y formación destinadas al control de inventarios y clasificación de controles de riesgo.

		<p>3. Horas de reuniones de charlas formales e informales, coaching y mentoring sobre control del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se destina tiempo y recursos económicos en la capacitación de los recursos humanos, que permite el adecuado control del riesgo.</p> <p>10% de las horas de reuniones de charlas formales e informales, destinadas al control del riesgo.</p>
RR 2.2	Supervisar la alineación operacional de los umbrales de tolerancia al riesgo	<p>1. Existe apoyo explícito de la dirección en la definición de indicadores de riesgo y definición de umbrales de tolerancia al riesgo.</p> <p>2. Existe un CMS de la organización con riesgos, tolerancia al riesgo y umbrales, disponible para la supervisión de la alineación operacional de los umbrales a la tolerancia al riesgo.</p>	<p>Existe una formación del personal en cuanto a riesgos, se considera la gestión de riesgos como una cuestión empresarial, capacitando y formando en el uso del conocimiento sobre riesgo, definición de indicadores y umbrales de tolerancia al riesgo.</p> <p>Se define un CMS centralizado con riesgos, tolerancia y umbrales, definiendo una base de conocimiento común a toda la organización.</p>
		<p>3. Existen reuniones de charlas y grupos de expertos para el logro de la aceptación de indicadores por parte de las áreas operativas y dirección.</p>	<p>Aplicando herramientas y técnicas de gestión del conocimiento se logra que los recursos humanos, definan la aceptación de indicadores para las áreas operativas y dirección.</p>
		<p>4. Horas de capacitación a la dirección en la definición de umbrales de tolerancia al riesgo y supervisión respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>La gestión de riesgos y definición de umbrales se considera una cuestión empresarial, por lo que se capacita y forma a los directores en el uso del conocimiento sobre riesgo.</p> <p>10% de las horas de capacitación se destinan a la definición de umbrales de tolerancia al resto y supervisión.</p>

RR 2.3	Responder a la exposición al riesgo descubierto y la oportunidad	<p>1. Existencia de conocimiento actualizado en el CMS para la respuesta al riesgo.</p> <p>2. Horas de reuniones de charlas formales e informales, coaching, mentoring sobre respuestas al riesgo descubierto y oportunidades respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existencia de un mapa de conocimiento que facilite el acceso y distribución de los riesgos descubiertos y oportunidades.</p>	<p>El CMS centralizado de la organización cuenta con conocimiento sobre la respuesta a riesgos.</p> <p>Existen políticas de respuesta a los riesgos que definen cuándo y cómo responder a estos. 10% de las horas de reuniones de charlas formales e informales, destinadas a respuestas al riesgo descubierto y oportunidades.</p> <p>Existen mapas de conocimiento con conocimiento que facilita la gestión de los riesgos descubiertos y oportunidades, a nivel de la organización, gestionados por el CKO.</p>
RR 2.4	Implementar los controles	<p>1. Existe un CMS actualizado con el conocimiento sobre controles de riesgo.</p> <p>2. Horas de reuniones de coaching, mentoring, charlas formales e informales, sobre implementación de controles respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El CMS centralizado de la organización cuenta con conocimiento sobre controles de riesgo.</p> <p>Se destina tiempo y recursos económicos que permite el adecuado control del riesgo. 10% de las horas de reuniones, destinadas a la implementación de control del riesgo.</p>
		<p>3. Existencia de un mapa de conocimientos actualizado que cuenta con la distribución del riesgo y controles existentes en la organización.</p>	<p>Existen mapas de conocimiento con conocimiento que facilita la distribución del riesgo y controles existentes, a nivel de la organización, gestionados por el CKO.</p>

		<p>4. Horas de capacitación y formación en la implementación de controles y uso de mapas de conocimiento para el mismo respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se destina tiempo y recursos económicos que permite el adecuado control del riesgo. 10% de las horas de capacitación y formación, destinadas a la implementación de controles y uso de mapas de conocimiento.</p>
RR 2.5	Informe del progreso del plan de acción de riesgos de TI	<p>1. Horas de capacitación al personal de TI y responsables del riesgo, en supervisión del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se destina tiempo y recursos económicos que permite la supervisión del plan de acción. 10% de las horas de capacitación, destinadas a la supervisión del plan de acción.</p>
		<p>2. Horas de reuniones de charlas, grupos de expertos, benchmarking en supervisión del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Horas de reuniones destinadas a la comunicación sobre el progreso del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se destina tiempo y recursos económicos que permite la adecuada supervisión del plan de acción. 10% de las horas de reuniones, destinadas a la supervisión del plan de acción.</p> <p>Se destina tiempo y recursos económicos que permite la adecuada comunicación del plan de acción. 10% de las horas de reuniones, destinadas a la comunicación del plan de acción.</p>
RR 3.1	Mantener los planes de respuesta a incidentes	<p>1. Existe un CMS actualizado de respuestas a incidentes, accesible a los responsables de TI y gestión del riesgo.</p>	<p>Existe un CMS de la organización donde se registra las respuestas a incidentes, que se desarrolla en cada área y es gestionada por el CKO.</p>

		<p>2. Horas de reuniones en charlas, grupos de expertos sobre comunicación y gestión de planes de respuesta respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican técnicas de gestión del conocimiento para optimizar la comunicación y gestión de planes de respuesta, que son gestionadas y facilitadas por el CKO. 10% de horas destinadas a reuniones en charlas, grupos de expertos sobre gestión de planes de respuesta y comunicación.</p>
RR 3.2	Supervisión de riesgos de TI	<p>1. Horas de capacitación a responsables del riesgo y auditores sobre supervisión de riesgo de TI respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de un CMS sobre riesgos y límites de la organización accesible a los responsables del riesgo y auditores.</p>	<p>Se dedica 10% de horas en capacitación y formación sobre supervisión del riesgo en TI.</p> <p>Existe un CMS de la organización donde se registra los riesgos y sus límites de tolerancia, que se desarrolla en cada área y es gestionada por el CKO.</p>
		<p>3. Horas de reuniones con grupos de expertos, charlas formales e informales sobre mejora en los riesgos de TI en base a los riesgos y límites tolerados respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican técnicas de gestión del conocimiento para optimizar la mejora en los riesgos de TI, según los riesgos y límites existentes en la base de la organización, que son gestionadas y facilitadas por el CKO. 10% de horas destinadas a reuniones en charlas, grupos de expertos sobre mejoras en los riesgos de TI.</p>

RR 3.3	Iniciar planes de respuesta a incidentes	<p>1. Horas de capacitación y formación de responsables de la gestión y el riesgo de la empresa, en el logro de las mejores respuestas de cada incidente y el uso del CMS de la organización para ello respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Los responsables de la gestión y del riesgo son capacitados para el logro de las mejores respuestas a incidentes haciendo uso del CMS de la organización. 10% de horas destinadas a capacitación y formación en el mejor uso de la información del CMS sobre respuestas de cada incidente de TI.</p>
		<p>2. Horas de reuniones en charlas formales e informales y benchmarking para lograr las mejores respuestas a incidentes y correcta distribución del conocimiento a los interesados respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican técnicas de gestión del conocimiento para el logro de las mejores respuestas a incidentes y su distribución en la organización, que son gestionadas y facilitadas por el CKO. 10% de horas destinadas a reuniones en charlas, benchmarking sobre mejores respuestas a incidentes de TI.</p>
		<p>3. Existencia de una base de conocimiento actualizada con categorías de hechos y respuestas.</p>	<p>Existe un CMS de la organización con las categorías de hechos y sus respuestas, que se desarrolla en cada área y es gestionada por el CKO.</p>
RR 3.4	Comunicar las lecciones aprendidas de eventos de riesgo	<p>1. Horas de capacitación y formación de responsables de TI y del riesgo de la empresa, en la identificación de las causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Los responsables de la gestión y del riesgo son capacitados en la identificación de causas de problemas, haciendo uso del CMS de la organización. 10% de horas destinadas a capacitación y formación en la identificación de causas de problemas.</p>

		<p>2. Horas de capacitación en charlas, grupos de expertos y benchmarking sobre identificación de causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existencia de un CMS actualizado con datos históricos y recientes de acontecimientos adversos y pérdidas.</p>	<p>Se aplican técnicas de gestión del conocimiento para la identificación de causas de problemas, que son gestionadas y facilitadas por el CKO. 10% de horas destinadas a reuniones, charlas, benchmarking sobre identificación de causas de problemas.</p> <p>Existe un CMS de la organización con información histórica y reciente de los acontecimientos adversos y pérdidas, que se desarrolla en cada área y es gestionada por el CKO.</p>
--	--	---	---

Nivel 3 de madurez

	Proceso	Indicador	Medida
RG	Proceso Gobierno del Riesgo		
RG 1.1	Desarrollar en una empresa el marco específico de gestión de riesgos de TI	<p>1. Porcentaje de variables de negocio para las cuales se ha identificado y registrado los puntos de TI que pueden aportar valor al negocio, para los cuales existe un análisis de tolerancia al riesgo. Registro de variables con tolerancia al riesgo en los rangos: 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>Se identifican y registran las variables de negocio y puntos de TI que pueden aportar valor al negocio con un análisis de tolerancia al riesgo alineado a TI y al negocio, en base a un inventario centralizado de riesgos de la organización, con el apoyo del CKO. Existe un registro de por lo menos el 60% de las variables identificadas y su tolerancia al riesgo.</p>
		<p>2. Existencia de mapas de conocimiento que vinculan los eventos de TI identificados.</p>	<p>Los mapas de conocimiento que vinculan los eventos de TI son desarrollados y actualizados rutinariamente en todas las áreas de la organización.</p>
RG 1.2	Proponer los umbrales de tolerancia de riesgos de TI	<p>1. Porcentaje de procesos de negocio que cuentan con medidas de riesgo y niveles de tolerancia asociados. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>60% de los procesos de negocio identificados, cuenta con medidas de riesgo y nivel de tolerancia definido.</p>
		<p>2. Existencia de recursos humanos capacitados para la definición de umbrales de tolerancia de riesgos de TI. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>La empresa se ocupa del desarrollo a largo plazo de las necesidades de personal, aplicando herramientas basadas en un plan estándar. Las habilidades son actualizadas rutinariamente en todas las áreas de la organización. 60% de los recursos destinados a la definición de umbrales capacitados.</p>

RG 1.3	Aprobar la tolerancia al riesgo	1. Existencia de mapas de conocimiento y base de conocimiento de todas las áreas de la empresa con umbrales de riesgo por área de negocio.	Los mapas y base de conocimiento con umbrales de riesgo son desarrollados y actualizados rutinariamente en todas las áreas de la organización.
RG 1.4	Alinear la política de riesgos de TI	1. Existencia de base de conocimiento de la organización con apetito al riesgo y tolerancia de cada área de negocio.	La base de conocimiento con apetito y tolerancia al riesgo es desarrollada y actualizada rutinariamente en todas las áreas de la organización.
		2. Nro. de horas de reunión de grupos de expertos por cada área sobre el número de áreas de negocio de la empresa, dedicados a la definición del apetito y tolerancia al riesgo de cada área respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Los requisitos de habilidad son actualizados rutinariamente en todas las áreas, por medio de herramientas y técnicas de gestión del conocimiento. 15% del tiempo de los recursos humanos es destinado a reuniones de grupos de expertos para la definición del apetito y tolerancia al riesgo.
RG 1.5	Promover los riesgos de TI – cultura consciente	1. Horas dedicadas en cursos sobre nro. de personas capacitadas en gestión del riesgo para cada área de negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	La gestión de riesgos se ve como facilitador de negocios y se entiende y gestiona la baja y alza de riesgos en TI. 15% del tiempo de los recursos humanos es destinado a cursos sobre gestión de riesgos.
		2. Existencia de base de conocimientos con registro de acciones y buenas prácticas en gestión del riesgo de cada área de negocio.	La base de conocimiento con registro de acciones y buenas prácticas en gestión del riesgo es desarrollada y actualizada rutinariamente en todas las áreas de la organización.
		3. Existencia del rol CKO dedicado a la comunicación de la política de gestión del riesgo en la organización.	El CKO comunica y relaciona la eficiencia y eficacia de los riesgos con los objetivos de negocio y plan estratégico de TI.

		4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	Las políticas y normas de la empresa reflejan la tolerancia al riesgo empresarial, se planifica los escenarios de riesgo considerando los riesgos de TI en toda la empresa. Existe un compromiso explícito de la alta gerencia y de todos los RRHH de la organización en cuanto a la gestión del conocimiento en riesgos.
RG 1.6	Promover una comunicación efectiva de los riesgos de TI	1. Existencia de un plan de comunicación de riesgos	La empresa se ocupa del desarrollo a largo plazo de las necesidades de personal con alto potencial en evaluación de riesgos y técnicas relacionadas. Se aplican herramientas de análisis de riesgo basadas en un plan estándar, e integradas con otras herramientas relacionadas, que se actualiza rutinariamente por medio de herramientas y técnicas de gestión del conocimiento.
		2. Existencia de una base de conocimiento organizacional accesible por responsables y directores con información sobre amenazas e impacto de riesgos por área. 3. Nro. de amenazas por área de negocio registradas en la base de conocimiento. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	La base de conocimiento con registro de amenazas e impacto de riesgos de la organización esta accesible para todos los responsables y directores. 60% de las amenazas identificadas son registradas en la base de conocimiento.

		4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	Las políticas y normas de la empresa reflejan la tolerancia al riesgo empresarial, se planifican los escenarios de riesgo considerando los riesgos de TI en toda la empresa. Existe un compromiso explícito de la alta gerencia y de todos los RRHH de la organización en cuanto a la gestión del conocimiento en riesgos.
RG 2.1	Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	<p>1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes.</p> <p>2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>Existe un plan de comunicación de riesgos de la organización el cual se desarrolla sistemáticamente aplicando técnicas y herramientas de gestión del conocimiento.</p> <p>60% de los roles o responsabilidades definidas en la empresa, participan en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno.</p>
RG 2.2	Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial	<p>1. Horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se desarrolla, capacita y forma al personal con planes a largo plazo en evaluación y gestión de riesgos. 15% del tiempo de los directores de TI y de las distintas áreas es destinado a la capacitación en definición de escalas, categorías y jerarquías de riesgos.</p>

		<p>2. Horas de reuniones dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se desarrolla, capacita y forma al personal con planes a largo plazo en evaluación y gestión de riesgos. 15% del tiempo de los directores de TI y de las distintas áreas es destinado a reuniones dedicadas a la coordinación para la definición de escalas, categorías y jerarquías de riesgos.</p>
RG 2.3	Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa	<p>3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p> <p>1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.</p>	<p>Asiste al menos al 60% de las reuniones de coordinación para la definición de escalas, categorías y jerarquías de riesgos, formando parte de una cultura de gestión del riesgo que es motivada por la organización.</p> <p>La base de conocimiento con registro de las prácticas en gestión del riesgo de la organización es desarrollada y esta accesible para todos los responsables y personal involucrado en dichas actividades.</p>
		<p>2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.</p>	<p>Los mapas de conocimiento con registro de buenas prácticas en gestión del riesgo son desarrollados y actualizados rutinariamente en todas las áreas de la organización.</p>
		<p>3. Porcentaje de recursos de la empresa capacitados o que asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>60% de los recursos de la empresa son capacitados o asisten a reuniones para la identificación y adquisición del conocimiento necesario para la alineación de las prácticas de TI con las de gestión del riesgo, relacionando los objetivos de negocio con el plan estratégico de TI.</p>

RG 2.4	Proporcionar recursos adecuados para la gestión de riesgos	<p>1. Nro. de horas en capacitación al personal de cada área en gestión del riesgo, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	Se desarrolla, capacita y forma al personal con planes a largo plazo en evaluación y gestión de riesgos. 15% del tiempo del personal destinado a la capacitación en riesgos.
		<p>2. Existencia de una base de conocimiento de la organización y mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	Los mapas y base de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable son desarrollados y actualizados rutinariamente en todas las áreas de la organización.
RG 2.5	Garantizar el aseguramiento independiente sobre la gestión de riesgos	<p>1. Existe una base de conocimiento con el registro del apetito al riesgo y tolerancia que permite la gestión del riesgo por parte del director de TI y director general.</p> <p>2. Existencia de mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	<p>La base de conocimiento con registro del apetito al riesgo y tolerancia es desarrollada y esta accesible para todos los responsables y personal involucrado en dichas actividades.</p> <p>Los mapas de conocimiento con registro de las relaciones de conocimiento existente por rol y responsable son desarrollados y actualizados rutinariamente en todas las áreas de la organización.</p>
		<p>3. Horas en capacitación de recursos humanos asegurando su independencia en la gestión de riesgos respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	Se desarrolla a largo plazo las necesidades de personal y su capacitación en gestión de riesgos. 15% del tiempo de los recursos humanos es destinado a la capacitación en riesgos.
RG 3.1	Ganancia de la gestión de compra para el enfoque de análisis de riesgos	<p>1. Existe una base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo.</p>	La base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo es desarrollada y esta accesible.

		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Los mapas de conocimiento con registro de las relaciones del conocimiento en riesgos son desarrollados y actualizados rutinariamente en todas las áreas de la organización.
		3. Horas de capacitación o reuniones que permitan interpretar los informes de análisis de riesgo y brechas existentes con el riesgo empresarial, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se aplican herramientas de análisis de riesgo basadas en un plan estándar, e integradas con otras herramientas relacionadas, 15% del tiempo de los recursos humanos es destinado a la capacitación en riesgos.
		4. Horas de capacitación en concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos de la empresa, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se ha creado una conciencia organizacional del riesgo, 15% del tiempo de los recursos humanos es destinado a la capacitación en riesgos.
RG 3.2	Aprobar el análisis de riesgos de TI	1. Existe una base de conocimiento única para las distintas áreas de la empresa accesible a todos los directores de área que permite registrar, transmitir y usar dicho conocimiento.	La base de conocimiento es desarrollada y esta accesible a todos los directores de área.
		2. Nro. de horas en capacitación y reuniones para la formación de los directores de área en la cultura de gestión del riesgo a través de la gestión del conocimiento respecto al total de horas de los directores. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se ha creado una cultura de gestión del riesgo, 15% del tiempo de los recursos humanos es destinado a la capacitación y reuniones en formación de los directores.

RG 3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.	La base de conocimiento que establece la incidencia del riesgo en TI en el negocio es desarrollada y esta accesible a todos los directores de la empresa.
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa. 3. Horas de capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Los mapas de conocimiento con registro de las relaciones del conocimiento en riesgos son desarrollados y actualizados rutinariamente en todas las áreas de la organización. Se ha creado una conciencia organizacional del riesgo, 15% del tiempo de los recursos humanos es destinado a la capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI.
RG 3.4	Aceptar los riesgos de TI	1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa. 2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	La base de conocimiento que establece la incidencia del riesgo en TI en el negocio es desarrollada y esta accesible a todos los directores de la empresa. Los mapas de conocimiento con registro de las relaciones del conocimiento en riesgos son desarrollados y actualizados rutinariamente en todas las áreas de la organización.

		<p>3. Horas de capacitación en formación al personal sobre aceptación y gestión del riesgo de TI para el negocio de cada área de la empresa respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se ha creado una conciencia organizacional del riesgo, 15% del tiempo de los recursos humanos es destinado a la capacitación en aceptación y gestión de riesgos de TI.</p>
RG 3.5	Priorizar actividades de respuesta de riesgos de TI	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa disponible para el director general y director de TI, que permita registrar métricas para el seguimiento del cumplimiento de las actividades de TI, así como priorización de las mismas, con información sobre el apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles.</p>	<p>La base de conocimiento donde se registran las métricas para el seguimiento del cumplimiento en TI, apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles, es desarrollada y esta accesible a todos los directores de la empresa.</p>
		<p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	<p>Los mapas de conocimiento con registro de las relaciones del conocimiento en riesgos son desarrollados y actualizados rutinariamente en todas las áreas de la organización.</p>
		<p>3. Horas de capacitación y formación al director general y de TI sobre seguimiento y planificación de riesgos en TI respecto al total de horas de los directores general y de TI.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se ha creado una conciencia organizacional del riesgo, 15% del tiempo del director general y de TI es destinado a la capacitación en seguimiento y planificación de riesgos de TI.</p>
RE	Gestión del Riesgo Proceso Evaluación del Riesgo (RE)		

RE 1.1	Establecer y mantener un modelo para la recolección de datos	<p>1. Existe apoyo explícito de la dirección para la concreción de la recopilación de datos para la formación de un repositorio único de conocimiento, así como en la culturización en gestión del conocimiento en la empresa.</p> <p>2. Existe una estrategia de adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.</p>	<p>Las políticas y normas de la empresa reflejan la tolerancia al riesgo empresarial. Se planifica la recopilación de datos y formación del repositorio único de conocimiento, así como el desarrollo a largo plazo de las necesidades de personal.</p> <p>Existe una estrategia de adquisición y retención del conocimiento para la organización, que se desarrolla activamente.</p>
		<p>3. Existe una implementación para la adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.</p>	<p>La adquisición y retención del conocimiento en la organización, se desarrolla activamente.</p>
		<p>4. Horas de capacitación y formación realizadas con el personal de la empresa respecto a la recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento en la organización.</p>	<p>Se ha creado una conciencia organizacional del riesgo, 15% del tiempo de los recursos humanos es destinado a la capacitación en recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento.</p>
RE 1.2	Recopilar datos sobre el entorno externo	<p>1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.</p>	<p>Se ha creado una conciencia organizacional del riesgo, 15% del tiempo de los recursos humanos es destinado a reuniones para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.</p>

RE 1.3	Recopilar datos sobre eventos de riesgo	<p>1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se ha creado una conciencia organizacional del riesgo, 15% del tiempo de los recursos humanos es destinado a reuniones para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.</p>
RE 1.4	Identificar factores de riesgo	<p>1. Horas de reuniones de charlas con expertos, coaching, comunidades de práctica realizadas por directivos de TI y de las restantes áreas de la empresa, aplicadas para la identificación de riesgos, asociados a proyectos, programas, servicios existentes y futuros, etc. que pueden generar eventos de riesgo, respecto al total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de una base de conocimiento organizacional donde se integra información sobre proyectos, programas, servicios e incidentes.</p>	<p>15% de las horas de los recursos son aplicados a reuniones para la identificación de riesgos.</p> <p>La base de conocimiento donde se integra la información sobre proyectos, programas, servicios e incidentes, es desarrollada activamente.</p>
RE 2.1	Definir Alcance del Análisis de Riesgo	<p>1. Horas de capacitación y formación al personal responsable de la gestión del riesgo y del negocio de la empresa, en cuanto a gestión y evaluación del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El proceso de gestión de riesgos se documenta y se gestiona cuantitativamente. Se aplican herramientas de análisis de riesgo basadas en un plan estándar, e integradas con otras herramientas relacionadas.</p> <p>15% de las horas dedicadas a la capacitación y formación en gestión y evaluación del riesgo.</p>

		<p>2. Horas de reuniones de charlas con expertos, benchmarking, realizadas con el personal responsable de la gestión del riesgo y el negocio sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El proceso de gestión de riesgos se documenta y se gestiona cuantitativamente. Se aplican herramientas de análisis de riesgo basadas en un plan estándar, e integradas con otras herramientas relacionadas. 15% de las horas dedicadas a la capacitación y formación en gestión y evaluación del riesgo.</p>
RE 2.2	Estimación de riesgos en TI	<p>1. Horas de capacitación y formación a los responsables del riesgo y de negocio de la empresa, sobre análisis de información de riesgo (factores, frecuencia, magnitud y tolerancia al riesgo) para la estimación y definición de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de un CMS disponible para el análisis en la estimación de riesgos.</p>	<p>Se mide y evalúa la eficiencia y eficacia de la gestión de riesgos y la respuesta al riesgo de forma cuantitativa. 15% de horas destinadas a capacitación y formación en estimación y definición de controles.</p> <p>El CMS donde se cuenta con las métricas para el seguimiento del cumplimiento en TI, apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles que facilitan el análisis para la estimación de riesgos, es desarrollado activamente.</p>

		<p>3. Horas de reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos en el CMS de la empresa.</p>	<p>Se realizan charlas con expertos para la optimización de la información del CMS y retroalimentación que permiten desarrollar activamente el conocimiento en estimación de riesgos.</p> <p>15% de las horas dedicadas a reuniones con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos.</p> <p>El CMS de la organización es actualizado activamente, con información sobre lecciones aprendidas y buenas prácticas que facilitan la estimación de riesgos.</p>
RE 2.3	Identificar las opciones de respuesta de riesgo	<p>1. Horas de capacitación y formación a los directivos y responsables del riesgo sobre identificación de respuestas de riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se mide y evalúa la eficiencia y eficacia de la gestión de riesgos y la respuesta al riesgo de forma cuantitativa. 15% de horas destinadas a capacitación y formación en identificación de respuestas de riesgo.</p>
		<p>2. Existencia de un CMS disponible para la consulta y actualización de respuestas de riesgo.</p>	<p>El CMS donde se cuenta con las opciones de respuesta al riesgo identificadas, es desarrollado activamente.</p>

		<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas de riesgos en el CMS de la empresa.</p>	<p>Se realizan charlas con expertos para la optimización de la información del CMS y retroalimentación que permiten desarrollar activamente el conocimiento en identificación de respuesta a los riesgos. 15% de las horas dedicadas a reuniones con expertos para la optimización y retroalimentación de la información disponible en el CMS para la identificación de respuestas a riesgos.</p> <p>El CMS de la organización es actualizado activamente, con información sobre lecciones aprendidas y buenas prácticas que facilitan la identificación de respuestas a riesgos.</p>
RE 2.4	Realizar una revisión por pares de los resultados de análisis de riesgos de TI	<p>1. Horas de capacitación y formación a los responsables del riesgo sobre la aplicación de técnicas para el análisis de riesgos de TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se mide y evalúa la eficiencia y eficacia de la gestión de riesgos y la respuesta al riesgo de forma cuantitativa. 15% de horas destinadas a capacitación y formación en aplicación de técnicas para el análisis de riesgos de TI.</p>
		<p>2. Existencia de un CMS disponible para la actualización de la información sobre riesgos de TI en la empresa.</p>	<p>El CMS donde se cuenta con las opciones de resultados de análisis de riesgo, es desarrollado activamente.</p>

		<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales, coaching en asignación de recursos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>4. Aplicación de sistemas expertos en la resolución de la asignación de recursos.</p>	<p>Se realizan charlas con expertos para la optimización de la información del CMS y retroalimentación que permiten desarrollar activamente el conocimiento en asignación de recursos. 15% de las horas dedicadas a reuniones con expertos para la optimización y retroalimentación de la información disponible en el CMS para la asignación de recursos.</p> <p>Se desarrolla activamente el uso de sistemas expertos en la resolución de la asignación de recursos.</p>
RE 3.1	Mapa de recursos de TI para procesos de negocio	<p>1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.</p>	<p>Los mapas de conocimiento con registro de las relaciones entre riesgos y actividades del negocio son desarrollados y actualizados rutinariamente en todas las áreas de la organización.</p>
		<p>3. Horas de capacitación y formación a los responsables del riesgo en la empresa, sobre uso y análisis de mapas de conocimiento respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El proceso de gestión del riesgo se documenta y se gestiona cuantitativamente, 15% del tiempo de los responsables del riesgo en la empresa es destinado a la capacitación en uso y análisis de mapas de conocimiento.</p>
RE 3.2	Determinar la criticidad de los negocios de recursos de TI	<p>1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.</p>	<p>Los mapas de conocimiento con registro de las relaciones entre riesgos y actividades del negocio son desarrollados y actualizados rutinariamente en todas las áreas de la organización.</p>

		<p>2. Horas de capacitación y formación a los responsables de la gestión de los recursos en las distintas áreas de la empresa, sobre la determinación de criticidad de los recursos según los requerimientos de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El proceso de gestión del riesgo se documenta y se gestiona cuantitativamente, 15% del tiempo de los responsables de la gestión de recursos en la empresa es destinado a la capacitación en determinación de criticidad de los recursos de TI.</p>
		<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales para la definición de la criticidad de los recursos de TI en cada área respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se realizan charlas con expertos para la optimización de la información del CMS y retroalimentación que permiten desarrollar activamente el conocimiento en la definición de la criticidad de los recursos de TI. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la optimización y retroalimentación de la información disponible en el CMS para la definición de la criticidad de los recursos de TI.</p>
		<p>4. Existencia de un CMS con información sobre riesgos, recursos y su criticidad.</p>	<p>El CMS donde se cuenta con la información de riesgos, recursos y su criticidad, es desarrollado activamente.</p>
RE 3.3	Entender las capacidades de TI	<p>1. Horas de capacitación y formación de los responsables de TI y responsables de cada área, para la evaluación de las capacidades disponibles y análisis de situación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El proceso de gestión del riesgo se documenta y se gestiona cuantitativamente, 15% del tiempo de los responsables de TI y de cada área en la empresa, es destinado a la capacitación en evaluación de capacidades disponibles y análisis de situación.</p>

		<p>2. Existe plan de capacitación de los responsables de cada área y de TI, sobre gestión del riesgo de TI.</p> <p>3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.</p>	<p>Existe un plan de capacitación sobre gestión de riesgo de TI, gestionado y desarrollado activamente por el CKO.</p> <p>Los mapas de conocimiento con registro de las capacidades y requerimientos en TI son desarrollados y actualizados rutinariamente en todas las áreas de la organización.</p>
		<p>4. Existencia de un CMS con información sobre las capacidades y requerimientos en TI de la empresa.</p>	<p>El CMS donde se cuenta con la información de capacidades y requerimientos de TI, es desarrollado activamente.</p>
		<p>5. Horas de reuniones de charlas formales e informales, consultas a expertos, sobre análisis de las capacidades existentes en TI y sus requerimientos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se realizan charlas formales e informales, consultas a expertos, optimizando la información del CMS que permite desarrollar activamente el conocimiento sobre capacidades y requerimientos de TI en toda la organización. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la optimización de la información disponible en el CMS para el análisis de las capacidades y requerimientos de TI.</p>
RE 3.4	Actualización de los componentes del escenario de riesgos de TI	<p>1. Horas de capacitación y formación de los responsables de negocio, riesgo y TI, para la evaluación de escenarios de riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El proceso de gestión del riesgo se documenta y se gestiona cuantitativamente, 15% del tiempo de los responsables de negocio, riesgo y TI, es destinado a la capacitación en evaluación de escenarios de riesgo.</p>

		<p>2. Existencia de un CMS con información sobre riesgos y distintos escenarios de riesgo.</p> <p>3. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre análisis de distintos escenarios de riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El CMS donde se cuenta con la información de riesgos y escenarios de riesgo, es desarrollado activamente.</p> <p>Se realizan charlas formales e informales, consultas a expertos, optimizando la información del CMS que permite desarrollar activamente el conocimiento sobre escenarios de riesgo en toda la organización. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la optimización de la información disponible en el CMS para el análisis de escenarios de riesgo.</p>
RE 3.5	Mantener los riesgos de TI y mapa de registro de riesgos de TI	<p>1. Horas de capacitación y formación de los responsables de negocio y TI, para la actualización de riesgos de TI y definición de perfil de riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El proceso de gestión del riesgo se documenta y se gestiona cuantitativamente, 15% del tiempo de los responsables de negocio, riesgo y TI, es destinado a la capacitación en definición de perfiles de riesgo.</p>
		<p>2. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre definición de perfil de riesgo de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se realizan charlas formales e informales, consultas a expertos, optimizando la información del CMS que permite desarrollar activamente el conocimiento sobre perfiles de riesgo en toda la organización. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la optimización de la información disponible en el CMS para la definición de perfiles de riesgo.</p>

		3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.	Los mapas de conocimiento con registro de las capacidades y requerimientos en TI son desarrollados y actualizados rutinariamente en todas las áreas de la organización.
RE 3.6	Diseñar y comunicar los indicadores de riesgo de TI	1. Existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo en TI en la empresa.	Las políticas y normas de la empresa reflejan el compromiso en la definición del diseño y comunicación de indicadores de riesgo en TI en toda la empresa.
		2. Horas de reuniones de charlas formales y consultas a expertos sobre difusión de indicadores de riesgo de la empresa respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se realizan charlas formales e informales, consultas a expertos, optimizando la información del CMS que permite desarrollar activamente el conocimiento sobre difusión de indicadores de riesgo en toda la organización. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la optimización de la difusión de indicadores.
		3. Existencia de conocimiento actualizado sobre buenas prácticas en difusión de indicadores en la base de conocimiento de la empresa.	El CMS donde se cuenta con la información de buenas prácticas en difusión de indicadores, es actualizado activamente.
RR	Gestión del Riesgo Proceso Respuesta del Riesgo (RR)		

RR 1.1	Informe de los resultados de análisis de riesgos de TI	<p>1. Horas de reuniones de charlas formales, consultas a expertos, coaching, mentoring sobre gestión de la comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se realizan charlas formales e informales, consultas a expertos, optimizando la gestión de la comunicación en toda la organización. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la optimización de la gestión de la comunicación.</p>
		<p>2. Horas de capacitación y formación sobre técnicas y herramientas de comunicación y coordinación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existe un CMS a nivel de la organización que permite adquirir el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, por parte de los responsables de negocio, riesgo y directores.</p>	<p>Las comunicaciones y coordinaciones se documentan y gestionan cuantitativamente, 15% del tiempo, es destinado a la capacitación en técnicas y herramientas de comunicación y coordinación.</p> <p>Los responsables de negocio, riesgo y directores acceden al CMS con información sobre el impacto de los acontecimientos y situaciones, que es desarrollado activamente.</p>
RR 1.2	Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	<p>1. Horas de reuniones de charlas formales e informales, consultas a expertos, coaching, mentoring sobre generación de informes y comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se realizan charlas formales e informales, consultas a expertos, optimizando la generación y distribución de informes en toda la organización. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la optimización en la generación y distribución de informes.</p>
		<p>2. Existe un CMS a nivel de la organización que permite la distribución de la información estratégica resultado de la gestión de riesgos.</p>	<p>El CMS cuenta con información estratégica sobre gestión de riesgo y estado de cumplimiento, que es desarrollado activamente.</p>

		3. Existencia de conocimiento actualizado en el CMS sobre lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados.	El CMS donde se cuenta con la información de buenas prácticas y lecciones aprendidas en generación de informes y distribución de resultados, es actualizado activamente.
RR 1.3	Interpretar resultados de la evaluación independiente de TI	1. Existencia de conocimiento actualizado en el CMS para el análisis de acciones correctivas e identificación de oportunidades de mejora.	El conocimiento sobre acciones correctivas e identificación de oportunidades de mejora del CMS es actualizado activamente.
		2. Horas de capacitación y formación de recursos humanos de la empresa en el análisis del conocimiento del CMS para la generación de planes de acción correctiva respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se planifica los escenarios de riesgo de TI en toda la empresa, se documentan y gestionan cuantitativamente, 15% del tiempo, es destinado a la capacitación en técnicas y herramientas de generación de planes de acción correctiva.
		3. Existencia de un plan de acción correctiva	La empresa se ocupa del desarrollo a largo plazo con un plan de acción correctiva, aplicando herramientas de análisis de riesgo basadas en un plan estándar, e integradas con otras herramientas relacionadas, que se actualiza rutinariamente por medio de herramientas y técnicas de gestión del conocimiento.

RR 1.4	Identificar TI Oportunidades relacionadas	<p>4. Horas de reuniones de charlas formales e informales, contacto personal, mentoring sobre el análisis de acciones correctivas y mejoras en la gestión del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>– 1. Horas de capacitación y formación de recursos humanos responsables de TI y del negocio de la empresa en el análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican técnicas y herramientas de gestión del conocimiento, mejorando el análisis de acciones correctivas y mejoras en la gestión del riesgo en toda la organización. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, contacto personal y mentoring para la mejora en el análisis de acciones correctivas y mejoras de gestión del riesgo.</p> <p>El conocimiento se desarrolla en todas en todas sus fases de socialización, externalización, internalización y combinación, por medio de una base de conocimiento común, logrando la transferencia del conocimiento y la determinación de las mejoras alternativas de uso de las TI. 15% de las horas de capacitación y formación, destinadas a la determinación de las mejores alternativas de uso de las TI.</p>
		<p>2. Horas de reuniones de charlas con expertos, coaching, benchmarking sobre optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican herramientas de análisis de riesgo en base a un plan estándar, facilitado por el uso de herramientas y técnicas de gestión del conocimiento. 15% de las horas de reuniones y charlas con expertos, coaching, benchmarking, destinadas a la optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas.</p>

RR 2.1	Controles del inventario	<p>1. Existencia de conocimiento actualizado en el CMS para el control de inventario de riesgos.</p> <p>2. Horas de capacitación y formación de recursos humanos de la empresa en el control de inventarios de riesgo y clasificación de controles respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Horas de reuniones de charlas formales e informales, coaching y mentoring sobre control del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El conocimiento se desarrolla en todas sus fases de socialización, externalización, internalización y combinación, por medio de una base de conocimiento común, que facilita el control de inventario de riesgos.</p> <p>Se facilita el control de inventarios y clasificación de controles aplicando herramientas y técnicas de gestión del conocimiento en base a un plan estándar. 15% de las horas destinadas a capacitación y formación, son destinados al control y clasificación de inventarios.</p> <p>Se facilita el control del riesgo aplicando herramientas y técnicas de gestión del conocimiento en base a un plan estándar. 15% de las horas destinadas a reuniones de charlas formales e informales, coaching y mentoring, son destinadas al control del riesgo.</p>
RR 2.2	Supervisar la alineación operacional de los umbrales de tolerancia al riesgo	<p>1. Existe apoyo explícito de la dirección en la definición de indicadores de riesgo y de definición de umbrales de tolerancia al riesgo.</p>	<p>Existe un compromiso explícito de la alta gerencia y de todos los recursos humanos de la organización en cuanto a la gestión del conocimiento en riesgos, apoyando la definición de indicadores de riesgo y umbrales de tolerancia.</p>

		2. Existe un CMS de la organización con riesgos, tolerancia al riesgo y umbrales, disponible para la supervisión de la alineación operacional de los umbrales a la tolerancia al riesgo.	El conocimiento sobre tolerancia y umbrales de riesgo, se desarrolla en todas las fases de gestión del conocimiento, haciendo uso de la base de conocimiento común.
		3. Existen reuniones de charlas y grupos de expertos para el logro de la aceptación de indicadores por parte de las áreas operativas y dirección respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Aplicando herramientas y técnicas de gestión del conocimiento en base a un plan estándar se logra la aceptación de indicadores en las áreas operativas y dirección. 10% de las horas destinadas a la aceptación de indicadores en las áreas operativas y dirección.
		4. Horas de capacitación a la dirección en la definición de umbrales de tolerancia al riesgo y supervisión respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Las políticas y normas de la empresa reflejan la tolerancia al riesgo empresarial. Se aplican herramientas y técnicas de gestión del conocimiento en base a un plan estándar. 15% de las horas de capacitación y formación, son destinados a la definición de umbrales de tolerancia al riesgo y supervisión.
RR 2.3	Responder a la exposición al riesgo descubierto y la oportunidad	1. Existencia de conocimiento actualizado en el CMS para la respuesta al riesgo.	El conocimiento sobre respuesta al riesgo, se desarrolla en todas las fases de gestión del conocimiento, haciendo uso de la base de conocimiento común.

		<p>2. Horas de reuniones de charlas formales e informales, coaching, mentoring sobre respuestas al riesgo descubierto y oportunidades respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Aplicando herramientas y técnicas de gestión del conocimiento en base a un plan estándar, se gestionan y analizan las respuestas al riesgo descubierto y oportunidades. 15% de las horas destinadas a reuniones con expertos y charlas formales e informales, coaching, mentoring son destinadas a respuestas a riesgos descubiertos y oportunidades.</p>
		<p>3. Existencia de un mapa de conocimiento que facilite el acceso y distribución de los riesgos descubiertos y oportunidades.</p>	<p>Los mapas de conocimiento con registro del riesgo descubierto y oportunidades son desarrollados y actualizados rutinariamente en todas las áreas de la organización.</p>
RR 2.4	Implementar los controles	<p>1. Existe un CMS actualizado con el conocimiento sobre controles de riesgo.</p>	<p>El conocimiento sobre controles de riesgo, se desarrolla en todas las fases de gestión del conocimiento, haciendo uso de la base de conocimiento común.</p>
		<p>2. Horas de reuniones de coaching, mentoring, charlas formales e informales, sobre implementación de controles respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existencia de un mapa de conocimientos actualizado que cuenta con la distribución del riesgo y controles existentes en la organización.</p>	<p>Herramientas y técnicas de gestión del conocimiento se aplican en base a un plan estándar, para la implementación de controles de riesgo. 15% de las horas destinadas a reuniones son destinadas a la implementación de controles.</p> <p>Los mapas de conocimiento con registro del riesgo son desarrollados y actualizados rutinariamente en todas las áreas de la organización, para la correcta distribución del riesgo y controles.</p>

		<p>4. Horas de capacitación y formación en la implementación de controles y uso de mapas de conocimiento para el mismo respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>15% de las horas de capacitación y formación, son destinados a la capacitación en implementación de controles y uso de mapas de conocimiento para tal fin.</p>
RR 2.5	Informe del progreso del plan de acción de riesgos de TI	<p>1. Horas de capacitación al personal de TI y responsables del riesgo, en supervisión del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de reuniones de charlas, grupos de expertos, benchmarking en supervisión del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Las políticas y normas de la empresa reflejan la tolerancia al riesgo empresarial. Se aplican herramientas y técnicas de gestión del conocimiento en base a un plan estándar. 15% de las horas de capacitación, son destinados a la supervisión del plan de acción.</p> <p>Herramientas y técnicas de gestión del conocimiento se aplican en base a un plan estándar, para la supervisión del plan de acción. 15% de las horas destinadas a reuniones sobre supervisión del plan de acción.</p>
		<p>3. Horas de reuniones destinadas a la comunicación sobre el progreso del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>15% de las horas destinadas a reuniones destinadas a la comunicación del plan de acción.</p>
RR 3.1	Mantener los planes de respuesta a incidentes	<p>1. Existe un CMS actualizado de respuestas a incidentes, accesible a los responsables de TI y gestión del riesgo.</p>	<p>El CMS cuenta con información sobre respuestas a incidentes, que es desarrollado activamente.</p>

		<p>2. Horas de reuniones en charlas, grupos de expertos sobre comunicación y gestión de planes de respuesta respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se realizan charlas, consultas a expertos, optimizando la gestión de planes de respuesta y su comunicación. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la optimización en la comunicación y gestión de planes de respuesta.</p>
RR 3.2	Supervisión de riesgos de TI	<p>1. Horas de capacitación a responsables del riesgo y auditores sobre supervisión de riesgo de TI respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de un CMS sobre riesgos y límites de la organización accesible a los responsables del riesgo y auditores.</p> <p>3. Horas de reuniones con grupos de expertos, charlas formales e informales sobre mejora en los riesgos de TI en base a los riesgos y límites tolerados respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican técnicas y herramientas de gestión del conocimiento para la mejora en la supervisión del riesgo en TI, 15% del tiempo, es destinado a la capacitación en supervisión del riesgo en TI.</p> <p>El CMS cuenta con información sobre riesgos y sus límites, que es desarrollado activamente.</p> <p>Se realizan charlas, consultas a expertos, optimizando la mejora en los riesgos de TI, haciendo uso del conocimiento del CMS sobre riesgos y límites tolerados. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la optimización en mejora de los riesgos de TI.</p>

RR 3.3	Iniciar planes de respuesta a incidentes	<p>1. Horas de capacitación y formación de responsables de la gestión y el riesgo de la empresa, en el logro de las mejores respuestas de cada incidente y el uso del CMS de la organización para ello respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Las comunicaciones y coordinaciones se documentan y gestionan cuantitativamente, 15% del tiempo, es destinado a la capacitación en técnicas y herramientas de comunicación y análisis de las mejores respuestas a cada incidente en TI.</p>
		<p>2. Horas de reuniones en charlas formales e informales y benchmarking para lograr las mejores respuestas a incidentes y correcta distribución del conocimiento a los interesados respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existencia de una base de conocimiento actualizada con categorías de hechos y respuestas.</p>	<p>Se realizan charlas, reuniones, benchmarking para el logro de la mejora en las respuestas a incidentes y su mejor distribución, haciendo uso del conocimiento del CMS. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, benchmarking para la mejora en la distribución del conocimiento y mejora en la respuesta a incidentes.</p> <p>El CMS cuenta con información sobre categorías de hechos y respuestas, que es desarrollado activamente.</p>
RR 3.4	Comunicar las lecciones aprendidas de eventos de riesgo	<p>1. Horas de capacitación y formación de responsables de TI y del riesgo de la empresa, en la identificación de las causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>15% del tiempo es destinado a la capacitación y formación en identificación de causas de problemas.</p>

		<p>2. Horas de capacitación en charlas, charlas, grupos de expertos y benchmarking sobre identificación de causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se realizan charlas, reuniones, benchmarking para el logro de la mejora en la identificación de causas de problemas, haciendo uso del conocimiento del CMS. 15% de las horas dedicadas a reuniones con expertos, charlas formales e informales, benchmarking para la mejora en la identificación de causas de problemas.</p>
		<p>3. Existencia de un CMS actualizado con datos históricos y recientes de acontecimientos adversos y pérdidas.</p>	<p>El CMS cuenta con información sobre información histórica y reciente de acontecimientos adversos y pérdidas, que es desarrollado activamente.</p>

Nivel 4 de madurez

	Proceso	Indicador	Medida
RG	Proceso Gobierno del Riesgo		
RG 1.1	Desarrollar en una empresa el marco específico de gestión de riesgos de TI	1. Porcentaje de variables de negocio para las cuales se ha identificado y registrado los puntos de TI que pueden aportar valor al negocio, para los cuales existe un análisis de tolerancia al riesgo. Registro de variables con tolerancia al riesgo en los rangos: 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	Se identifican y registran las variables de negocio y puntos de TI que pueden aportar valor al negocio con un análisis de tolerancia al riesgo aplicando procesos de mejora continua. Existe un registro de por lo menos el 80% de las variables identificadas y su tolerancia al riesgo.
		2. Existencia de mapas de conocimiento que vinculan los eventos de TI identificados.	Los mapas de conocimiento que vinculan los eventos de TI, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.
RG 1.2	Proponer los umbrales de tolerancia de riesgos de TI	1. Porcentaje de procesos de negocio que cuentan con medidas de riesgo y niveles de tolerancia asociados. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	80% de los procesos de negocio identificados, cuenta con medidas de riesgo y nivel de tolerancia definido.
		2. Existencia de recursos humanos capacitados para la definición de umbrales de tolerancia de riesgos de TI. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	En un proceso de mejora continua la empresa gestiona las capacidades de los recursos para la definición de umbrales. 80% de los recursos humanos destinados a la definición de umbrales es capacitado.
RG 1.3	Aprobar la tolerancia al riesgo	1. Existencia de mapas de conocimiento y base de conocimiento de todas las áreas de la empresa con umbrales de riesgo por área de negocio.	Los mapas y base de conocimiento que vinculan los eventos de TI, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.

RG 1.4	Alinear la política de riesgos de TI	1. Existencia de base de conocimiento de la organización con apetito al riesgo y tolerancia de cada área de negocio.	La base de conocimiento con apetito al riesgo y tolerancia de cada área, se utiliza en toda la organización y es mejorada en forma permanente a través de un proceso de mejora continua.
RG 1.5	Promover los riesgos de TI – cultura consciente	<p>2. Nro. de horas de reunión de grupos de expertos por cada área sobre el número de áreas de negocio de la empresa, dedicados a la definición del apetito y tolerancia al riesgo de cada área respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>1. Horas dedicadas en cursos sobre nro. de personas capacitadas en gestión del riesgo para cada área de negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>La alta gerencia considera en sus decisiones todos los aspectos de la gestión del riesgo y conocimiento. 20% de las horas de recursos humanos destinadas a reuniones de grupos de expertos para la definición del apetito y tolerancia al riesgo.</p> <p>Se capacita los recursos humanos de forma sistemática y planificada. 20% de las horas de recursos humanos de la empresa, destinados a cursos sobre gestión del riesgo.</p>
		<p>2. Existencia de base de conocimientos con registro de acciones y buenas prácticas en gestión del riesgo de cada área de negocio.</p> <p>3. Existencia del rol CKO dedicado a la comunicación de la política de gestión del riesgo en la organización.</p>	<p>La base de conocimiento con registro de acciones y buenas prácticas en gestión de riesgos de cada área, se utiliza en toda la organización y es mejorada en forma permanente a través de un proceso de mejora continua.</p> <p>Se aplica una gestión del conocimiento definida y gestionada por el CKO, fomentando y manteniendo la cultura de gestión del riesgo en toda la organización.</p>

		4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	Existe un compromiso de la alta gerencia y cultura organizacional que facilita y exige formalmente la promoción de la política de gestión del riesgo en toda la organización, aplicando herramientas y técnicas de gestión del conocimiento que mejor se ajustan.
RG 1.6	Promover una comunicación efectiva de riesgos de TI	<p>1. Existencia de un plan de comunicación de riesgos</p> <p>2. Existencia de una base de conocimiento organizacional accesible por responsables y directores con información sobre amenazas e impacto de riesgos por área.</p>	
		3. Nro. de amenazas por área de negocio registradas en la base de conocimiento. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	80% de las amenazas identificadas son registradas en la base de conocimiento.
RG 2.1	Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	<p>4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.</p> <p>1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes.</p>	Existe un plan de comunicación de riesgos de la organización el cual se desarrolla sistemáticamente en un proceso de mejora continua, aplicando técnicas y herramientas de gestión del conocimiento que brindan los mejores resultados en la comunicación de riesgos.

<p>RG 2.2</p>	<p>Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial</p>	<p>2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p> <p>1. Horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>80% de los roles o responsabilidades definidas en la empresa, participan en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno.</p> <p>Existe un compromiso de la alta gerencia y cultura organizacional que permiten gestionar la capacitación constante de los recursos humanos en la gestión del riesgo alineado al negocio. 20% de las horas de los directores de TI y de las distintas áreas son destinados a la capacitación en definición de escalas, categorías y jerarquías de riesgos.</p>
		<p>2. Horas de reuniones dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Existe un compromiso de la alta gerencia y cultura organizacional que permiten gestionar la capacitación constante de los recursos humanos en la gestión del riesgo alineado al negocio. 20% de las horas de los directores de TI y de las distintas áreas son destinados a reuniones para la definición de escalas, categorías y jerarquías de riesgos.</p>

		<p>3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>Asiste al menos al 80% de las reuniones de coordinación entre directores para la definición de escalas categorías y jerarquías de riesgos, la cual es instrumentada formalmente por la empresa como parte de un proceso de mejora continua de la gestión en riesgos.</p>
RG 2.3	Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa	<p>1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.</p> <p>2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.</p>	<p>La base de conocimiento con registro de las buenas prácticas en gestión de riesgos, se utiliza en toda la organización y es mejorada en forma permanente a través de un proceso de mejora continua.</p> <p>Los mapas de conocimiento con registro de buenas prácticas en gestión del riesgo, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.</p>
		<p>3. Porcentaje de recursos de la empresa capacitados o que asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	<p>80% de los recursos de la empresa son capacitados y/o asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las de gestión del riesgo, por medio de una capacitación constante alineada con el negocio y gestionada por el CKO.</p>

<p>RG 2.4</p>	<p>Proporcionar recursos adecuados para la gestión de riesgos</p>	<p>1. Nro. de horas en capacitación al personal de cada área en gestión del riesgo, respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de una base de conocimiento de la organización y mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	<p>Existe un compromiso de la alta gerencia y cultura organizacional que permiten gestionar la capacitación constante de los recursos humanos en la gestión del riesgo alineado al negocio. 20% de las horas del personal destinados a la capacitación en riesgos.</p> <p>Los mapas y base de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.</p>
<p>RG 2.5</p>	<p>Garantizar el aseguramiento independiente sobre la gestión de riesgos</p>	<p>1. Existe una base de conocimiento con el registro del apetito al riesgo y tolerancia que permite la gestión del riesgo por parte del director de TI y director general.</p> <p>2. Existencia de mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	<p>La base de conocimiento con registro del apetito al riesgo y tolerancia, se utiliza y es mejorada en forma permanente a través de un proceso de mejora continua.</p> <p>Los mapas de conocimiento con registro de las relaciones de conocimiento existente por rol y responsable, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.</p>
		<p>3. Horas en capacitación de recursos humanos asegurando su independencia en la gestión de riesgos respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Existe un compromiso de la alta gerencia y cultura organizacional que permiten gestionar la capacitación constante de los recursos humanos en la gestión del riesgo alineado al negocio. 20% de las horas de los recursos humanos son destinados a la capacitación en gestión de riesgos.</p>

RG 3.1	Ganancia de la gestión de compra para el enfoque de análisis de riesgos	1. Existe una base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo.	La base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo, se utiliza y es mejorada en forma permanente a través de un proceso de mejora continua.
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Los mapas de conocimiento con registro de las relaciones de conocimiento en riesgos, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.
		3. Horas de capacitación o reuniones que permitan interpretar los informes de análisis de riesgo y brechas existentes con el riesgo empresarial, respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	La empresa exige formalmente la mejora continua de la gestión de las capacidades de los riesgos de TI basada en objetivos claramente definidos. Existe un seguimiento en tiempo real de los eventos y excepciones de control. 20% de las horas de los recursos humanos son destinados a la capacitación en gestión de riesgos.

		<p>4. Horas de capacitación en concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos de la empresa, respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se capacita los recursos humanos de forma sistemática y planificada. Se exige la mejora continua en la gestión de las capacidades de los riesgos de TI basada en objetivos claramente definidos de personal y de organización, que se logra aplicando técnicas y herramientas de gestión del conocimiento. 20% de las horas de los recursos humanos aplicados a la concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos.</p>
RG 3.2	Aprobar el análisis de riesgos de TI	<p>1. Existe una base de conocimiento única para las distintas áreas de la empresa accesible a todos los directores de área que permite registrar, transmitir y usar dicho conocimiento.</p> <p>2. Nro. de horas en capacitación y reuniones para la formación de los directores de área en la cultura de gestión del riesgo a través de la gestión del conocimiento respecto al total de horas de los directores.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>La base de conocimiento se utiliza y es mejorada en forma permanente a través de un proceso de mejora continua.</p> <p>Se capacita a los directores de área de forma sistemática y planificada. Se exige la mejora continua en la gestión de las capacidades de los directores, que se logra aplicando técnicas y herramientas de gestión del conocimiento. 20% de las horas de los directores son aplicados a la formación de una cultura de gestión del riesgo.</p>
RG 3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.</p>	<p>La base de conocimiento que establece la incidencia del riesgo en TI en el negocio se utiliza y es mejorada en forma permanente a través de un proceso de mejora continua.</p>

		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Los mapas de conocimiento con registro de las relaciones de conocimiento en riesgos, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.
RG 3.4	Aceptar los riesgos de TI	3. Horas de capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe un compromiso de la alta gerencia y cultura organizacional que permiten gestionar la capacitación constante de los recursos humanos en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio. 20% de las horas de los recursos humanos son destinados a la capacitación.
		1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.	La base de conocimiento que establece la incidencia del riesgo en TI en el negocio se utiliza y es mejorada en forma permanente a través de un proceso de mejora continua.
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Los mapas de conocimiento con registro de las relaciones de conocimiento en riesgos, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.
		3. Horas de capacitación en formación al personal sobre aceptación y gestión del riesgo de TI para el negocio de cada área de la empresa respecto al total de horas de los recursos humanos de la empresa. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe un compromiso de la alta gerencia y cultura organizacional que permiten gestionar la capacitación constante de los recursos humanos en aceptación y gestión de riesgo de TI para el negocio. 20% de las horas de los recursos humanos son destinados a la capacitación.

RG 3.5	Priorizar actividades de respuesta de riesgos de TI	1. Existe una base de conocimiento para la gestión del riesgo en la empresa disponible para el director general y director de TI, que permita registrar métricas para el seguimiento del cumplimiento de las actividades de TI, así como priorización de las mismas, con información sobre el apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles.	La base de conocimiento con métricas para el seguimiento del cumplimiento de las actividades de TI, apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles, se utiliza y es mejorada en forma permanente a través de un proceso de mejora continua.
		2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.	Los mapas de conocimiento con registro de las relaciones de conocimiento en riesgos, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.
		3. Horas de capacitación y formación al director general y de TI sobre seguimiento y planificación de riesgos en TI respecto al total de horas de los directores general y de TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe un compromiso de la alta gerencia que permiten gestionar la capacitación constante del director general y de TI en seguimiento y planificación de la gestión de riesgos en TI para el negocio. 20% de las horas del director general y de TI son destinados a la capacitación.
RE	Gestión del Riesgo Proceso Evaluación del Riesgo (RE)		
RE 1.1	Establecer y mantener un modelo para la recolección de datos	1. Existe apoyo explícito de la dirección para la concreción de la recopilación de datos para la formación de un repositorio único de conocimiento, así como en la culturización en gestión del conocimiento en la empresa.	Se exige formalmente la mejora continua de la recogida de datos. Existe un compromiso de la alta gerencia y cultura organizacional que permiten gestionar la capacitación constante de los recursos humanos en la gestión del riesgo alineado al negocio.

		2. Existe una estrategia de adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	Existe una estrategia de adquisición y retención del conocimiento para la organización, que se desarrolla siguiendo un proceso de mejora continua.
		3. Existe una implementación para la adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.	Se implementa la estrategia de adquisición y retención siguiendo un proceso de mejora continua.
RE 1.2	Recopilar datos sobre el entorno externo	4. Horas de capacitación y formación realizadas con el personal de la empresa respecto a la recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento en la organización. 1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.	Existe un compromiso de la alta gerencia que permiten gestionar la capacitación constante del personal respecto a la recopilación eficiente de datos. 20% de las horas del personal son destinados a la capacitación en recopilación eficiente de datos para facilitar la toma de decisiones. 20% de las horas del personal son destinados a reuniones aplicadas a la recolección de datos para facilitar la toma de decisiones.
RE 1.3	Recopilar datos sobre eventos de riesgo	1. Horas de reuniones de benchmarking, charlas informales y con expertos, por área de la empresa, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	20% de las horas del personal son destinados a reuniones aplicadas a la recolección de datos para facilitar la toma de decisiones.

RE 1.4	Identificar factores de riesgo	<p>1. Horas de reuniones de charlas con expertos, coaching, comunidades de práctica realizadas por directivos de TI y de las restantes áreas de la empresa, aplicadas para la identificación de riesgos, asociados a proyectos, programas, servicios existentes y futuros, etc. que pueden generar eventos de riesgo, respecto al total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>20% de las horas de los recursos son aplicados a reuniones para la identificación de riesgos.</p>
RE 2.1	Definir Alcance del Análisis de Riesgo	<p>1. Horas de capacitación y formación al personal responsable de la gestión del riesgo y del negocio de la empresa, en cuanto a gestión y evaluación del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>La base de conocimiento donde se integra información sobre proyectos, programas, servicios e incidentes, se utiliza y es mejorada en forma permanente a través de un proceso de mejora continua.</p> <p>La empresa exige la mejora continua en la evaluación de los riesgos. Las políticas de empresa y las normas siguen reflejando la tolerancia al riesgo empresarial mientras aumenta la eficiencia. 20% de las horas dedicadas a la capacitación y formación en gestión y evaluación del riesgo.</p>

		<p>2. Horas de reuniones de charlas con expertos, benchmarking, realizadas con el personal responsable de la gestión del riesgo y el negocio sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>La empresa exige la mejora continua en la evaluación de los riesgos. Las políticas de empresa y las normas siguen reflejando la tolerancia al riesgo empresarial mientras aumenta la eficiencia. 20% de las horas dedicadas a la capacitación y formación en gestión y evaluación del riesgo.</p>
RE 2.2	Estimación de riesgos en TI	<p>1. Horas de capacitación y formación a los responsables del riesgo y de negocio de la empresa, sobre análisis de información de riesgo (factores, frecuencia, magnitud y tolerancia al riesgo) para la estimación y definición de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de un CMS disponible para el análisis en la estimación de riesgos.</p>	<p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la estimación y definición de controles. 20% de horas destinadas a capacitación y formación en estimación y definición de controles.</p> <p>El CMS que establece la incidencia del riesgo en TI en el negocio se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.</p>
		<p>3. Horas de reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la estimación de riesgos, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos.</p>

		4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos en el CMS de la empresa.	Se exige formalmente la mejora continua de la recogida de datos, análisis y estimación de riesgos apoyados por herramientas automatizadas que mejoran la evaluación de riesgos para inteligentemente asumir riesgos adicionales y aprovechar oportunidades optimizando los factores de tiempo y recursos económicos.
RE 2.3	Identificar las opciones de respuesta de riesgo	1. Horas de capacitación y formación a los directivos y responsables del riesgo sobre identificación de respuestas de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la identificación de respuestas de riesgo. 20% de horas destinadas a capacitación y formación en identificación de respuestas de riesgo.
		2. Existencia de un CMS disponible para la consulta y actualización de respuestas de riesgo.	El CMS que cuenta con las respuestas de riesgo se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.
		3. Horas de reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la identificación de respuestas a riesgos, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la identificación de respuestas a riesgos.

		4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas de riesgos en el CMS de la empresa.	Las estrategias de respuesta de riesgo son aplicadas de manera integral, justificada y controles costo-eficacia mitigan la exposición al riesgo en forma continua.
RE 2.4	Realizar una revisión por pares de los resultados de análisis de riesgos de TI	1. Horas de capacitación y formación a los responsables del riesgo sobre la aplicación de técnicas para el análisis de riesgos de TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en el análisis de riesgo. 20% de horas destinadas a capacitación y formación en aplicación de técnicas para el análisis de riesgos de TI.
		2. Existencia de un CMS disponible para la actualización de la información sobre riesgos de TI en la empresa.	El CMS que cuenta con las respuestas de riesgo se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.
		3. Horas de reuniones de charlas con expertos, charlas formales e informales, coaching en asignación de recursos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la asignación de recursos, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en la asignación de recursos.
		4. Aplicación de sistemas expertos en la resolución de la asignación de recursos.	Se desarrolla activamente y de forma integral, por medio de un proceso de mejora continua, el uso de sistemas expertos en la resolución de la asignación de recursos.

RE 3.1	Mapa de recursos de TI para procesos de negocio	1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.	Los mapas de conocimiento con registro de las relaciones entre riesgos y actividades de negocio, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.
		3. Horas de capacitación y formación a los responsables del riesgo en la empresa, sobre uso y análisis de mapas de conocimiento respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe un compromiso de la alta gerencia que permiten gestionar la capacitación constante de los responsables del riesgo. 20% de las horas de los responsables del riesgo son destinados a la capacitación y formación.
RE 3.2	Determinar la criticidad de los negocios de recursos de TI	1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.	Los mapas de conocimiento con registro de las relaciones entre riesgos y actividades de negocio, se utilizan en toda la organización y son mejorados en forma permanente a través de un proceso de mejora continua.
		2. Horas de capacitación y formación a los responsables de la gestión de los recursos en las distintas áreas de la empresa, sobre la determinación de criticidad de los recursos según los requerimientos de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe un compromiso de la alta gerencia que permite gestionar la capacitación constante de los responsables de la gestión de recursos. 20% de las horas de los responsables de la gestión de recursos son destinados a la capacitación y formación en la determinación de criticidad de los recursos de TI.

		<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales para la definición de la criticidad de los recursos de TI en cada área respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la determinación de la criticidad de los recursos de TI, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en la definición de la criticidad de los recursos de TI.</p>
		<p>4. Existencia de un CMS con información sobre riesgos, recursos y su criticidad.</p>	<p>El CMS que cuenta con los riesgos, recursos y su criticidad se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.</p>
RE 3.3	Entender las capacidades de TI	<p>1. Horas de capacitación y formación de los responsables de TI y responsables de cada área, para la evaluación de las capacidades disponibles y análisis de situación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Existe un compromiso de la alta gerencia que permite gestionar la capacitación constante de los responsables de cada área. 20% de las horas de los responsables de cada área, son destinados a la capacitación y formación en la evaluación de las capacidades disponibles en TI y análisis de situación.</p>
		<p>2. Existe plan de capacitación de los responsables de cada área y de TI, sobre gestión del riesgo de TI.</p>	<p>Existe un plan de capacitación de los responsables de cada área y de TI, gestionado, desarrollado e integrado, por el CKO siguiendo un proceso de mejora continua.</p>

		3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.	Los mapas de conocimiento con registro de las capacidades y requerimientos de TI en la organización, son utilizados y mejorados en forma permanente a través de un proceso de mejora continua.
		4. Existencia de un CMS con información sobre las capacidades y requerimientos en TI de la empresa.	El CMS que cuenta con las capacidades y requerimientos de TI de la organización, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.
		5. Horas de reuniones de charlas formales e informales, consultas a expertos, sobre análisis de las capacidades existentes en TI y sus requerimientos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en el análisis de las capacidades y requerimientos de TI, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en el análisis de las capacidades y requerimientos de TI.
RE 3.4	Actualización de los componentes del escenario de riesgos de TI	1. Horas de capacitación y formación de los responsables de negocio, riesgo y TI, para la evaluación de escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe un compromiso de la alta gerencia que permite gestionar la capacitación constante de los responsables de cada área. 20% de las horas de los responsables de cada área, son destinados a la capacitación y formación en la evaluación de escenarios de riesgo.

		2. Existencia de un CMS con información sobre riesgos y distintos escenarios de riesgo.	El CMS que cuenta con los riesgos y distintos escenarios de riesgo de la organización, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.
RE 3.5	Mantener los riesgos de TI y mapa de registro de riesgos de TI	3. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre análisis de distintos escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en el análisis de escenarios de riesgo, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en el análisis de escenarios de riesgo.
		1. Horas de capacitación y formación de los responsables de negocio y TI, para la actualización de riesgos de TI y definición de perfil de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Existe un compromiso de la alta gerencia que permite gestionar la capacitación constante de los responsables de cada área. 20% de las horas de los responsables de cada área, son destinados a la capacitación y formación en la actualización de riesgos y definición de perfiles de riesgo.
		2. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre definición de perfil de riesgo de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la definición de perfiles de riesgo, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en la definición de perfiles de riesgo.

		3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.	Los mapas de conocimiento con registro de las capacidades y requerimientos de TI en la organización, son utilizados y mejorados en forma permanente a través de un proceso de mejora continua.
RE 3.6	Diseñar y comunicar los indicadores de riesgo de TI	<p>1. Existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo en TI en la empresa.</p> <p>2. Horas de reuniones de charlas formales y consultas a expertos sobre difusión de indicadores de riesgo de la empresa respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Existe un compromiso de la alta gerencia y cultura organizacional que facilita y exige formalmente el diseño y la comunicación de indicadores del riesgo en toda la organización, aplicando herramientas y técnicas de gestión del conocimiento que mejor se ajustan.</p> <p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la difusión de indicadores de riesgo, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en la difusión de indicadores de riesgo.</p>
		3. Existencia de conocimiento actualizado sobre buenas prácticas en difusión de indicadores en la base de conocimiento de la empresa.	El conocimiento sobre buenas prácticas en difusión de indicadores de la organización, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.
RR	Gestión del Riesgo Proceso Respuesta del Riesgo (RR)		

RR 1.1	Informe de los resultados de análisis de riesgos de TI	<p>1. Horas de reuniones de charlas formales, consultas a expertos, coaching, mentoring sobre gestión de la comunicación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la gestión de la comunicación, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en la gestión de la comunicación.</p>
		<p>2. Horas de capacitación y formación sobre técnicas y herramientas de comunicación y coordinación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Existe un compromiso de la alta gerencia que permite gestionar la capacitación constante. 20% de las horas, son destinados a la capacitación y formación en técnicas y herramientas de comunicación y coordinación.</p>
		<p>3. Existe un CMS a nivel de la organización que permite adquirir el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, por parte de los responsables de negocio, riesgo y directores.</p>	<p>El CMS que cuenta con los impactos positivos y negativos de los acontecimientos y situaciones de riesgo de la organización, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.</p>
RR 1.2	Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	<p>1. Horas de reuniones de charlas formales e informales, consultas a expertos, coaching, mentoring sobre generación de informes y comunicación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la generación de informes y su comunicación, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en la generación de informes y su comunicación.</p>

		2. Existe un CMS a nivel de la organización que permite la distribución de la información estratégica resultado de la gestión de riesgos.	El CMS que cuenta con la información estratégica de la gestión de riesgos de la organización, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.
		3. Existencia de conocimiento actualizado en el CMS sobre lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados.	El CMS que cuenta con lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados de la organización, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.
RR 1.3	Interpretar resultados de la evaluación independiente de TI	<p>1. Existencia de conocimiento actualizado en el CMS para el análisis de acciones correctivas e identificación de oportunidades de mejora.</p> <p>2. Horas de capacitación y formación de recursos humanos de la empresa en el análisis del conocimiento del CMS para la generación de planes de acción correctiva respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Conocimiento sobre acciones correctivas e identificación de oportunidades de mejora, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.</p> <p>20% de las horas, son destinados a la capacitación y formación en análisis del conocimiento del CMS para la generación de planes de acción correctiva.</p>
		3. Existencia de un plan de acción correctiva	Existe un plan de acción correctiva de riesgos de la organización el cual se desarrolla sistemáticamente en un proceso de mejora continua, aplicando técnicas y herramientas de gestión del conocimiento que brindan los mejores resultados en la comunicación de riesgos.

		<p>4. Horas de reuniones de charlas formales e informales, contacto personal, mentoring sobre el análisis de acciones correctivas y mejoras en la gestión del riesgo respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>El análisis de acciones correctivas y mejoras en la gestión del riesgo son mejorados en forma continua aplicando herramientas y técnicas de gestión del conocimiento, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en el análisis de acciones correctivas y mejoras en la gestión del riesgo.</p>
RR 1.4	Identificar TI Oportunidades relacionadas	<p>– 1. Horas de capacitación y formación de recursos humanos responsables de TI y del negocio de la empresa en el análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Los responsables de las decisiones disfrutaban de la transparencia en los riesgos de TI y disponen de la mejor información acerca de las probabilidades de pérdida, riesgos y oportunidades. 20% de horas de capacitación y formación, destinadas al análisis del conocimiento del CMS para determinar las mejores alternativas de uso de las TI.</p>
		<p>2. Horas de reuniones de charlas con expertos, coaching, benchmarking sobre optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se mide y se mejora la gestión del riesgo y el conocimiento, aplicando técnicas y herramientas que permite la mejor asignación del riesgo, así como el uso, desarrollo y distribución de lecciones aprendidas y buenas prácticas. 20% de las horas en reuniones de charlas con expertos, coaching, benchmarking destinadas a la optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas.</p>

RR 2.1	Controles inventario	del	1. Existencia de conocimiento actualizado en el CMS para el control de inventario de riesgos.	El CMS se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua, permitiendo la optimización del control de inventario de riesgos.
			2. Horas de capacitación y formación de recursos humanos de la empresa en el control de inventarios de riesgo y clasificación de controles respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Los responsables de las decisiones disfrutan de la transparencia en los riesgos de TI y disponen de la mejor información acerca del inventario y controles de riesgo. 20 % de horas de capacitación y formación, destinadas al control de inventarios y clasificación de controles.
			3. Horas de reuniones de charlas formales e informales, coaching y mentoring sobre control del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	Se mide y se mejora la gestión del riesgo y el conocimiento, aplicando técnicas y herramientas que permiten el mejor control del riesgo. 20 % de las horas en reuniones de charlas formales e informales, coaching y mentoring destinadas a la optimización en el control del riesgo.
RR 2.2	Supervisar alineación operacional de los umbrales de tolerancia al riesgo	la	1. Existe apoyo explícito de la dirección en la definición de los indicadores de riesgo y definición de umbrales de tolerancia al riesgo. 2. Existe un CMS de la organización con riesgos, tolerancia al riesgo y umbrales, disponible para la supervisión de la alineación operacional de los umbrales a la tolerancia al riesgo.	Existe un compromiso de la alta gerencia y cultura organizacional que facilita y exige formalmente la definición de indicadores y umbrales de tolerancia al riesgo en toda la organización. El CMS se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua, permitiendo la supervisión y alineamiento de la tolerancia al riesgo y umbrales.

		<p>3. Existen reuniones de charlas y grupos de expertos para el logro de la aceptación de indicadores por parte de las áreas operativas y dirección respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se mide y se mejora la gestión del riesgo y el conocimiento, aplicando técnicas y herramientas que permiten el mejor control del riesgo. 20 % de las horas en reuniones con expertos y charlas formales e informales, son destinadas al logro de la aceptación de indicadores.</p>
RR 2.3	<p>Responder a la exposición al riesgo descubierto y la oportunidad</p>	<p>4. Horas de capacitación a la dirección en la definición de umbrales de tolerancia al riesgo y supervisión respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Los responsables de las decisiones disfrutan de la transparencia en los riesgos de TI y disponen de la mejor información. 20 % de horas de capacitación y formación, destinadas a la definición de umbrales de tolerancia y supervisión.</p>
		<p>1. Existencia de conocimiento actualizado en el CMS para la respuesta al riesgo.</p>	<p>El conocimiento sobre respuesta al riesgo del CMS se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.</p>
		<p>2. Horas de reuniones de charlas formales e informales, coaching, mentoring sobre respuestas al riesgo descubierto y oportunidades respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se mide y se mejora la gestión del riesgo y el conocimiento, aplicando técnicas y herramientas que permiten el mejor control del riesgo. 20 % de las horas en reuniones con expertos y charlas formales e informales, son destinadas a la gestión de las respuestas al riesgo descubierto y oportunidades.</p>
		<p>3. Existencia de un mapa de conocimiento que facilite el acceso y distribución de los riesgos descubiertos y oportunidades.</p>	<p>Los mapas de conocimiento son utilizados y mejorados en forma permanente a través de un proceso de mejora continua, que facilita el acceso y distribución de los riesgos descubiertos y oportunidades.</p>

RR 2.4	Implementar los controles	<p>1. Existe un CMS actualizado con el conocimiento sobre controles de riesgo.</p> <p>2. Horas de reuniones de coaching, mentoring, charlas formales e informales, sobre implementación de controles respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>CMS se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.</p> <p>Se mide y se mejora la gestión del riesgo y el conocimiento, aplicando técnicas y herramientas que permiten el mejor control del riesgo. 20 % de las horas en reuniones, son destinadas a la implementación de controles.</p>
		<p>3. Existencia de un mapa de conocimientos actualizado que cuenta con la distribución del riesgo y controles existentes en la organización.</p>	<p>Los mapas de conocimiento son utilizados y mejorados en forma permanente a través de un proceso de mejora continua, que facilita el acceso y distribución de los riesgos y controles existentes.</p>
		<p>4. Horas de capacitación y formación en la implementación de controles y uso de mapas de conocimiento para el mismo respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Los responsables de las decisiones disfrutan de la transparencia en los riesgos de TI y disponen de la mejor información acerca de la implementación de controles y uso de mapas. 20 % de horas de capacitación y formación, destinadas a la implementación de controles y uso de mapas de conocimiento.</p>
RR 2.5	Informe del progreso del plan de acción de riesgos de TI	<p>1. Horas de capacitación al personal de TI y responsables del riesgo, en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Los responsables de las decisiones disfrutan de la transparencia en los riesgos de TI y disponen de la mejor información acerca de la supervisión de controles. 20 % de horas de capacitación y formación, destinadas a la supervisión del plan de acción.</p>

		<p>2. Horas de reuniones de charlas, grupos de expertos, benchmarking en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Horas de reuniones destinadas a la comunicación sobre el progreso del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se mide y se mejora la gestión del riesgo y el conocimiento, aplicando técnicas y herramientas que permiten la mejor supervisión del plan de acción. 20 % de las horas en reuniones, son destinadas a la supervisión del plan de acción.</p> <p>Se mide y se mejora la gestión del riesgo y el conocimiento, aplicando técnicas y herramientas que permiten la mejor comunicación del progreso del plan de acción. 20 % de las horas en reuniones, son destinadas a la comunicación sobre el progreso del plan de acción.</p>
RR 3.1	Mantener los planes de respuesta a incidentes	1. Existe un CMS actualizado de respuestas a incidentes, accesible a los responsables de TI y gestión del riesgo.	El CMS que cuenta con la información sobre respuestas a incidentes de la organización, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.
		<p>2. Horas de reuniones en charlas, grupos de expertos sobre comunicación y gestión de planes de respuesta respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la comunicación y gestión de planes de respuesta, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en la gestión de planes de respuesta y su comunicación.</p>

RR 3.2	Supervisión de riesgos de TI	<p>1. Horas de capacitación a responsables del riesgo y auditores sobre supervisión de riesgo de TI respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>20% de las horas, son destinados a la capacitación y formación en supervisión del riesgo en TI.</p>
		<p>2. Existencia de un CMS sobre riesgos y límites de la organización accesible a los responsables del riesgo y auditores.</p>	<p>El CMS que cuenta con la información sobre riesgos y límites de la organización, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.</p>
		<p>3. Horas de reuniones con grupos de expertos, charlas formales e informales sobre mejora en los riesgos de TI en base a los riesgos y límites tolerados respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la mejora de los riesgos en TI, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, para la mejora en los riesgos en TI.</p>
RR 3.3	Iniciar planes de respuesta a incidentes	<p>1. Horas de capacitación y formación de responsables de la gestión y el riesgo de la empresa, en el logro de las mejores respuestas de cada incidente y el uso del CMS de la organización para ello respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>20% de las horas, son destinadas a la capacitación y formación en el logro de mejores respuestas a incidentes, así como el uso del conocimiento del CMS.</p>

		<p>2. Horas de reuniones en charlas formales e informales y benchmarking para lograr las mejores respuestas a incidentes y correcta distribución del conocimiento a los interesados respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la comunicación y logro de las mejores respuestas a incidentes, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, benchmarking para la mejora en la distribución del conocimiento y logro de mejores respuestas a incidentes.</p>
		<p>3. Existencia de una base de conocimiento actualizada con categorías de hechos y respuestas.</p>	<p>El CMS que cuenta con la información sobre categorías de hechos y respuestas de la organización, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.</p>
RR 3.4	Comunicar las lecciones aprendidas de eventos de riesgo	<p>1. Horas de capacitación y formación de responsables de TI y del riesgo de la empresa, en la identificación de las causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>20% de las horas, son destinadas a la capacitación y formación en la identificación de causas de problemas, así como el uso del conocimiento del CMS.</p>
		<p>2. Horas de reuniones y charlas, grupos de expertos y benchmarking sobre identificación de causas de problemas respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>Se aplican herramientas y técnicas de gestión del conocimiento para el logro de la mejora continua en la identificación de causas de problemas, haciendo uso de la información disponible en el CMS. 20% de las horas dedicadas a reuniones con expertos, charlas formales e informales, benchmarking para la mejora en la identificación de causas de problemas.</p>

		3. Existencia de un CMS actualizado con datos históricos y recientes de acontecimientos adversos y pérdidas.	El CMS que cuenta con la información histórica y reciente de acontecimientos adversos y pérdidas, se utiliza y es mejorado en forma permanente a través de un proceso de mejora continua.
--	--	--	---

Justificación de Indicadores

A continuación se detalla para cada indicador, la referencia bibliográfica y argumentación teórica que justifica su definición y uso, como métrica para el modelo.

	Proceso	Indicador	Justificación
RG RG 1.1	Proceso Gobierno del Riesgo Desarrollar en una empresa el marco específico de gestión de riesgos de TI	1. Porcentaje de variables de negocio para las cuales se ha identificado y registrado los puntos de TI que pueden aportar valor al negocio, para los cuales existe un análisis de tolerancia al riesgo. Registro de variables con tolerancia al riesgo en los rangos: 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	(Métrica del proceso RG1, Risk IT[11])
RG 1.2	Proponer los umbrales de tolerancia de riesgos de TI	2. Existencia de mapas de conocimiento que vinculan los eventos de TI identificados. 1. Porcentaje de procesos de negocio que cuentan con medidas de riesgo y niveles de tolerancia asociados. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	(Herramienta de representación del conocimiento y su distribución, Davenport y Prusak [67][70]) (Métrica de actividades y dominio RG1, Risk IT[11])

		2. Existencia de recursos humanos capacitados para la definición de umbrales de tolerancia de riesgos de TI. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	(Métrica de actividades y dominio RG1, Risk IT[11])
RG 1.3	Aprobar la tolerancia al riesgo	1. Existencia de mapas de conocimiento y base de conocimiento de todas las áreas de la empresa con umbrales de riesgo por área de negocio.	(Herramienta de representación del conocimiento y su distribución, Davenport y Prusak [67][70])
RG 1.4	Alinear la política de riesgos de TI	1. Existencia de base de conocimiento de la organización con apetito al riesgo y tolerancia de cada área de negocio.	(Técnica de gestión del conocimiento para la persistencia y distribución del conocimiento [65][67])
		2. Nro. de horas de reunión de grupos de expertos por cada área sobre el número de áreas de negocio de la empresa, dedicados a la definición del apetito y tolerancia al riesgo de cada área.	(Herramienta de gestión del conocimiento, Probst [65][67])
RG 1.5	Promover los riesgos de TI – cultura consciente	1. Horas dedicadas en cursos sobre nro. de personas capacitadas en gestión del riesgo para cada área de negocio. 2. Existencia de base de conocimientos con registro de acciones y buenas prácticas en gestión del riesgo de cada área de negocio.	(Herramienta de gestión del conocimiento, Probst [65][67]) (Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		3. Existencia del rol CKO dedicado a la comunicación de la política de gestión del riesgo en la organización.	(Factor de gestión del conocimiento encargado de la dirección de la gestión del conocimiento [52][67])

		4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	(Métrica de actividades RG1, Risk IT[11])
RG 1.6	Promover una comunicación efectiva de los riesgos de TI	1. Existencia de un plan de comunicación de riesgos 2. Existencia de una base de conocimiento organizacional accesible por responsables y directores con información sobre amenazas e impacto de riesgos por área.	(Asociado a métrica de actividades RG1, Risk IT[11]) (Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		3. Nro. de amenazas por área de negocio registradas en la base de conocimiento. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	(Asociado a métrica de actividades RG1, Risk IT[11])
		4. Existencia de compromiso explícito de la alta gerencia en la promoción de la política de gestión del riesgo en la organización.	(Métrica de actividades RG1, Risk IT[11])
RG 2.1	Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	1. Existencia de un plan de comunicación de gestión de riesgos aplicado a toda la empresa según los roles y responsabilidades existentes.	(Asociado a métrica de actividades RG2, Risk IT[11])
		2. Porcentaje de participación de cada rol o responsabilidad con respecto al total de los empleados de la empresa, en la definición y evaluación de las relaciones riesgo-recompensa y riesgo-retorno. 1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%	(Asociado a métrica de actividades RG2, Risk IT[11])

RG 2.2	Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial	<p>1. Horas dedicadas en capacitación de los directores de TI y de las distintas áreas para la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Asociado a métricas de proceso y dominio RG2, Risk IT[11])
		<p>2. Horas de reuniones dedicadas en coordinación entre los directores de TI y de las distintas áreas, en la definición de escalas, categorías y jerarquías de riesgos, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])
		<p>3. Porcentaje de participación de cada director en las reuniones de coordinación entre directores para la definición de escalas, categorías y jerarquías de riesgos.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])
RG 2.3	Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa	<p>1. Existe una base de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		<p>2. Existencia de mapas de conocimiento con el registro de las prácticas en gestión del riesgo de la empresa.</p>	(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])

		<p>3. Porcentaje de recursos de la empresa capacitados o que asisten a reuniones sobre identificación y adquisición del conocimiento necesario para alinear las prácticas de TI con las prácticas en gestión del riesgo.</p> <p>1. 0-20% 2. 20-40% 3. 40-60% 4. 60-100%</p>	(Asociado a métricas de proceso y dominio RG2, Risk IT[11])
RG 2.4	Proporcionar recursos adecuados para la gestión de riesgos	<p>1. Nro. de horas en capacitación al personal de cada área en gestión del riesgo, respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Existencia de una base de conocimiento de la organización y mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	(Asociado a métricas de proceso y dominio RG2, Risk IT[11]) (Herramienta y técnica para la representación, persistencia y distribución del conocimiento [67][70])
RG 2.5	Garantizar el aseguramiento independiente sobre la gestión de riesgos	<p>1. Existe una base de conocimiento con el registro del apetito al riesgo y tolerancia que permite la gestión del riesgo por parte del director de TI y director general.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		<p>2. Existencia de mapas de conocimiento con las relaciones de conocimiento existente en la empresa por rol y responsable.</p>	(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])

		<p>3. Horas en capacitación de recursos humanos asegurando su independencia en la gestión de riesgos respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Asociado a métricas de proceso y dominio RG2, Risk IT[11])
RG 3.1	Ganancia de la gestión de compra para el enfoque de análisis de riesgos	<p>1. Existe una base de conocimiento con registro de la calidad esperada en la toma de decisiones en gestión del riesgo.</p> <p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	<p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p> <p>(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])</p>
		<p>3. Horas de capacitación o reuniones que permitan interpretar los informes de análisis de riesgo y brechas existentes con el riesgo empresarial, respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])
		<p>4. Horas de capacitación en concientización y comprensión sobre la importancia de la gestión de riesgos de TI en la gestión de riesgos de la empresa, respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
RG 3.2	Aprobar el análisis de riesgos de TI	<p>1. Existe una base de conocimiento única para las distintas áreas de la empresa accesible a todos los directores de área que permite registrar, transmitir y usar dicho conocimiento.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])

		<p>2. Nro. de horas en capacitación y reuniones para la formación de los directores de área en la cultura de gestión del riesgo a través de la gestión del conocimiento respecto al total de horas de los directores.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
RG 3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		<p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p> <p>3. Horas de capacitación en concientización y comprensión de la importancia de la gestión de riesgos de TI para el negocio respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70]) (Factor relativo a la mejora en la gestión del conocimiento [52][67])
RG 3.4	Aceptar los riesgos de TI	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa que establezca la incidencia del riesgo en TI en el negocio, accesible por todos los directores de la empresa.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		<p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])

		<p>3. Horas de capacitación en formación al personal sobre aceptación y gestión del riesgo de TI para el negocio de cada área de la empresa respecto al total de horas de los recursos humanos de la empresa.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
RG 3.5	Priorizar actividades de respuesta de riesgos de TI	<p>1. Existe una base de conocimiento para la gestión del riesgo en la empresa disponible para el director general y director de TI, que permita registrar métricas para el seguimiento del cumplimiento de las actividades de TI, así como priorización de las mismas, con información sobre el apetito y tolerancia al riesgo, controles, capacidades y recursos disponibles.</p> <p>2. Existencia de mapas de conocimiento con el registro de las relaciones del conocimiento en riesgos de la empresa.</p>	<p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p> <p>(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])</p>
		<p>3. Horas de capacitación y formación al director general y de TI sobre seguimiento y planificación de riesgos en TI respecto al total de horas de los directores general y de TI.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
RE	Gestión del Riesgo Proceso Evaluación del Riesgo (RE)		

RE 1.1	Establecer y mantener un modelo para la recolección de datos	<p>1. Existe apoyo explícito de la dirección para la concreción de la recopilación de datos para la formación de un repositorio único de conocimiento, así como en la culturización en gestión del conocimiento en la empresa.</p> <p>2. Existe una estrategia de adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.</p>	<p>(Asociado a la necesidad de una herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [52][67])</p> <p>(Asociado a métricas de actividades de RE1, Risk IT[11])</p>
		<p>3. Existe una implementación para la adquisición y retención del conocimiento relevante para la gestión del riesgo en todas las áreas de la organización.</p>	<p>(Asociado a métricas de actividades de RE1, Risk IT[11])</p>
		<p>4. Horas de capacitación y formación realizadas con el personal de la empresa respecto a la recopilación eficiente de datos para facilitar la toma de decisiones sobre la implementación de una estrategia de gestión del conocimiento en la organización, respecto al total de horas del personal.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p>
RE 1.2	Recopilar datos sobre el entorno externo	<p>1. Horas de reuniones de benchmarking, charlas informales y con expertos, aplicadas para la recolección de datos que faciliten la toma de decisiones para la prevención de riesgos en TI.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Herramienta de gestión del conocimiento, Probst [65][67])</p>

		<p>2. Horas de reuniones de charlas con expertos, benchmarking, realizadas con el personal responsable de la gestión del riesgo y el negocio sobre análisis de riesgo y ponderación sobre el alcance del análisis de riesgo de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])
RE 2.2	Estimación de riesgos en TI	<p>1. Horas de capacitación y formación a los responsables del riesgo y de negocio de la empresa, sobre análisis de información de riesgo (factores, frecuencia, magnitud y tolerancia al riesgo) para la estimación y definición de controles respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
		<p>2. Existencia de un CMS disponible para el análisis en la estimación de riesgos.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		<p>3. Horas de reuniones de charlas con expertos para la optimización y retroalimentación de la información disponible en el CMS para la estimación de riesgos respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])

		4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la estimación de riesgos en el CMS de la empresa.	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
RE 2.3	Identificar las opciones de respuesta de riesgo	1. Horas de capacitación y formación a los directivos y responsables del riesgo sobre identificación de respuestas de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
		2. Existencia de un CMS disponible para la consulta y actualización de respuestas de riesgo.	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		3. Horas de reuniones de charlas con expertos, charlas formales e informales, para la identificación de respuestas a riesgos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	(Herramienta de gestión del conocimiento, Probst [65][67])
RE 2.4	Realizar una revisión por pares de los resultados de análisis de riesgos de TI	4. Existencia de información actualizada sobre lecciones aprendidas y buenas prácticas respecto a la identificación de respuestas de riesgos en el CMS de la empresa. 1. Horas de capacitación y formación a los responsables del riesgo sobre la aplicación de técnicas para el análisis de riesgos de TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67]) (Factor relativo a la mejora en la gestión del conocimiento [52][67])

		<p>2. Existencia de un CMS disponible para la actualización de la información sobre riesgos de TI en la empresa.</p> <p>3. Horas de reuniones de charlas con expertos, charlas formales e informales, coaching en asignación de recursos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p> <p>(Herramienta de gestión del conocimiento, Probst [65][67])</p>
		<p>4. Aplicación de sistemas expertos en la resolución de la asignación de recursos.</p>	<p>(Técnica de gestión del conocimiento que aplica al área de conocimiento de asignación de recursos [52][67])</p>
RE 3.1	Mapa de recursos de TI para procesos de negocio	<p>1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.</p> <p>2. Horas de capacitación y formación a los responsables del riesgo en la empresa, sobre uso y análisis de mapas de conocimiento respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])</p> <p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p>
RE 3.2	Determinar la criticidad de negocios de los recursos de TI	<p>1. Existencia de mapas de conocimiento con el registro de las relaciones entre riesgos y actividades de negocio.</p>	<p>(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])</p>

		<p>2. Horas de capacitación y formación a los responsables de la gestión de los recursos en las distintas áreas de la empresa, sobre la determinación de criticidad de los recursos según los requerimientos de la organización respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p>
		<p>3. Horas de reuniones de charlas con expertos, charlas formales e informales para la definición de la criticidad de los recursos de TI en cada área respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Herramienta de gestión del conocimiento, Probst [65][67])</p>
		<p>4. Existencia de un CMS con información sobre riesgos, recursos y su criticidad.</p>	<p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p>
RE 3.3	Entender las capacidades de TI	<p>1. Horas de capacitación y formación de los responsables de TI y responsables de cada área, para la evaluación de las capacidades disponibles y análisis de situación respecto del total de horas de estos recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p>
		<p>2. Existe plan de capacitación de los responsables de cada área y de TI, sobre gestión del riesgo de TI.</p>	<p>(Relativo a factor para la mejora en la gestión del conocimiento [52][67])</p>

		<p>3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.</p> <p>4. Existencia de un CMS con información sobre las capacidades y requerimientos en TI de la empresa.</p> <p>5. Horas de reuniones de charlas formales e informales, consultas a expertos, sobre análisis de las capacidades existentes en TI y sus requerimientos respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])</p> <p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p> <p>(Herramienta de gestión del conocimiento, Probst [65][67])</p>
RE 3.4	Actualización de los componentes del escenario de riesgos de TI	<p>1. Horas de capacitación y formación de los responsables de negocio, riesgo y TI, para la evaluación de escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
		<p>2. Existencia de un CMS con información sobre riesgos y distintos escenarios de riesgo.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		<p>3. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre análisis de distintos escenarios de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])

RE 3.5	Mantener los riesgos de TI y mapa de registro de riesgos de TI	<p>1. Horas de capacitación y formación de los responsables de negocio y TI, para la actualización de riesgos de TI y definición de perfil de riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de reuniones de charlas formales e informales, consultas a expertos, benchmarking sobre definición de perfil de riesgo de la organización respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existencia de mapas de conocimiento con el registro de las capacidades en TI y requerimientos existentes.</p>	<p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p> <p>(Herramienta de gestión del conocimiento, Probst [65][67])</p> <p>(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])</p>
RE 3.6	Diseñar y comunicar los indicadores de riesgo de TI	<p>1. Existe compromiso explícito de la dirección en el diseño y comunicación de indicadores de riesgo en TI en la empresa.</p>	<p>(Métrica de proceso RE3, Risk IT[11])</p>
		<p>2. Horas de reuniones de charlas formales y consultas a expertos sobre difusión de indicadores de riesgo de la empresa respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Herramienta de gestión del conocimiento, Probst [65][67])</p>
		<p>3. Existencia de conocimiento actualizado sobre buenas prácticas en difusión de indicadores en la base de conocimiento de la empresa.</p>	<p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p>

RR	Gestión del Riesgo Proceso Respuesta del Riesgo (RR)		
RR 1.1	Informe de los resultados de análisis de riesgos de TI	1. Horas de reuniones de charlas formales, consultas a expertos, coaching, mentoring sobre gestión de la comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	(Herramienta de gestión del conocimiento, Probst [65][67])
		2. Horas de capacitación y formación sobre técnicas y herramientas de comunicación y coordinación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	(Factor relativo a la mejora en la gestión del conocimiento de [52][67])
		3. Existe un CMS a nivel de la organización que permite adquirir el conocimiento del impacto positivo o negativo de los acontecimientos y situaciones, por parte de los responsables de negocio, riesgo y directores.	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
RR 1.2	Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento	1. Horas de reuniones de charlas formales e informales, consultas a expertos, coaching, mentoring sobre generación de informes y comunicación respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	(Herramienta de gestión del conocimiento, Probst [65][67])
		2. Existe un CMS a nivel de la organización que permite la distribución de la información estratégica resultado de la gestión de riesgos.	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])

		3. Existencia de conocimiento actualizado en el CMS sobre lecciones aprendidas y buenas prácticas en la generación de informes y distribución de resultados.	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
RR 1.3	Interpretar resultados de la evaluación independiente de TI	1. Existencia de conocimiento actualizado en el CMS para el análisis de acciones correctivas e identificación de oportunidades de mejora.	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		2. Horas de capacitación y formación de recursos humanos de la empresa en el análisis del conocimiento del CMS para la generación de planes de acción correctiva respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
		3. Existencia de un plan de acción correctiva	(Métrica del dominio RR1, Risk IT[11])
		4. Horas de reuniones de charlas formales e informales, contacto personal, mentoring sobre el análisis de acciones correctivas y mejoras en la gestión del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%	(Herramienta de gestión del conocimiento, Probst [65][67])

RR 1.4	Identificar Oportunidades relacionadas TI	<p>– 1. Horas de capacitación y formación de recursos humanos responsables de TI y del negocio de la empresa en el análisis del conocimiento del CMS para la determinación de mejores alternativas de uso de las TI respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
		<p>2. Horas de reuniones de charlas con expertos, coaching, benchmarking sobre optimización en la asignación del riesgo, lecciones aprendidas y buenas prácticas respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])
RR 2.1	Controles del inventario	<p>1. Existencia de conocimiento actualizado en el CMS para el control de inventario de riesgos.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		<p>2. Horas de capacitación y formación de recursos humanos de la empresa en el control de inventarios de riesgo y clasificación de controles respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
		<p>3. Horas de reuniones de charlas formales e informales, coaching y mentoring sobre control del riesgo respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])

RR 2.2	Supervisar la alineación operacional de los umbrales de tolerancia al riesgo	<p>1. Existe apoyo explícito de la dirección en la definición de indicadores de riesgo y definición de umbrales de tolerancia al riesgo.</p> <p>2. Existe un CMS de la organización con riesgos, tolerancia al riesgo y umbrales, disponible para la supervisión de la alineación operacional de los umbrales a la tolerancia al riesgo.</p>	<p>(Métrica de actividades RR2, Risk IT[11])</p> <p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p>
RR 2.3	Responder a la exposición al riesgo descubierto y la oportunidad	<p>3. Existen reuniones de charlas y grupos de expertos para el logro de la aceptación de indicadores por parte de las áreas operativas y dirección.</p> <p>4. Horas de capacitación a la dirección en la definición de umbrales de tolerancia al riesgo y supervisión respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>1. Existencia de conocimiento actualizado en el CMS para la respuesta al riesgo.</p> <p>2. Horas de reuniones de charlas formales e informales, coaching, mentoring sobre respuestas al riesgo descubierto y oportunidades respecto del total de horas de estos recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>3. Existencia de un mapa de conocimiento que facilite el acceso y distribución de los riesgos descubiertos y oportunidades.</p>	<p>(Herramienta de gestión del conocimiento, Probst [65][67])</p> <p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p> <p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p> <p>(Herramienta de gestión del conocimiento, Probst [65][67])</p> <p>(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])</p>

RR 2.4	Implementar los controles	<p>1. Existe un CMS actualizado con el conocimiento sobre controles de riesgo.</p> <p>2. Horas de reuniones de coaching, mentoring, charlas formales e informales, sobre implementación de controles respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p> <p>(Herramienta de gestión del conocimiento, Probst [65][67])</p>
		<p>3. Existencia de un mapa de conocimientos actualizado que cuenta con la distribución del riesgo y controles existentes en la organización.</p> <p>4. Horas de capacitación y formación en la implementación de controles y uso de mapas de conocimiento para el mismo respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Herramienta para la representación del conocimiento y su distribución, Davenport y Prusak [67][70])</p> <p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p>
RR 2.5	Informe del progreso del plan de acción de riesgos de TI	<p>1. Horas de capacitación al personal de TI y responsables del riesgo, en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de reuniones de charlas, grupos de expertos, benchmarking en supervisión del plan de acción respecto del total de horas de los recursos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p> <p>(Herramienta de gestión del conocimiento, Probst [65][67])</p>

		<p>3. Horas de reuniones destinadas a la comunicación sobre el progreso del plan de acción respecto del total de horas de los recursos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])
RR 3.1	Mantener los planes de respuesta a incidentes	<p>1. Existe un CMS actualizado de respuestas a incidentes, accesible a los responsables de TI y gestión del riesgo.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
		<p>2. Horas de reuniones en charlas, grupos de expertos sobre comunicación y gestión de planes de respuesta respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])
RR 3.2	Supervisión de riesgos de TI	<p>1. Horas de capacitación a responsables del riesgo y auditores sobre supervisión de riesgo de TI respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
		<p>2. Existencia de un CMS sobre riesgos y límites de la organización accesible a los responsables del riesgo y auditores.</p> <p>3. Horas de reuniones con grupos de expertos, charlas formales e informales sobre mejora en los riesgos de TI en base a los riesgos y límites tolerados respecto al total de horas de los recursos humanos.</p> <p>1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])</p> <p>(Herramienta de gestión del conocimiento, Probst [65][67])</p>

RR 3.3	Iniciar planes de respuesta a incidentes	<p>1. Horas de capacitación y formación de responsables de la gestión y el riesgo de la empresa, en el logro de las mejores respuestas de cada incidente y el uso del CMS de la organización para ello respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Factor relativo a la mejora en la gestión del conocimiento [52][67])
		<p>2. Horas de reuniones en charlas formales e informales y benchmarking para lograr las mejores respuestas a incidentes y correcta distribución del conocimiento a los interesados respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	(Herramienta de gestión del conocimiento, Probst [65][67])
		<p>3. Existencia de una base de conocimiento actualizada con categorías de hechos y respuestas.</p>	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
RR 3.4	Comunicar las lecciones aprendidas de eventos de riesgo	<p>1. Horas de capacitación y formación de responsables de TI y del riesgo de la empresa, en la identificación de las causas de problemas respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p> <p>2. Horas de capacitación en charlas, grupos de expertos y benchmarking sobre identificación de causas de problemas respecto al total de horas de los recursos humanos. 1. 0-5% 2. 5-10% 3. 10-15% 4. 15-20%</p>	<p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p> <p>(Factor relativo a la mejora en la gestión del conocimiento [52][67])</p>

	3. Existencia de un CMS actualizado con datos históricos y recientes de acontecimientos adversos y pérdidas.	(Técnica de gestión del conocimiento para facilitar la persistencia y distribución del conocimiento [52][67])
--	--	---