UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSTGRADO

MODELO DE GESTIÓN DE RIESGOS DE TI ENFOCADO EN ESTÁNDARES ADAPTADOS PARA CONTRIBUIR EN LA PROTECCIÓN DEL ACTIVO DE TI EN EL SECTOR DE DISTRIBUIDORAS DE LA REGIÓN LAMBAYEQUE

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR

WILSON EVERTH CRUZ CABRERA

ASESOR

GREGORIO MANUEL LEÓN TENORIO

https://orcid.org/0000-0002-9650-4427

Chiclayo, 2019

MODELO DE GESTIÓN DE RIESGOS DE TI ENFOCADO EN ESTÁNDARES ADAPTADOS PARA CONTRIBUIR EN LA PROTECCIÓN DEL ACTIVO DE TI EN EL SECTOR DE DISTRIBUIDORAS DE LA REGIÓN LAMBAYEQUE

PRESENTADA POR:

WILSON EVERTH CRUZ CABRERA

A la Escuela de Posgrado de la

Universidad Católica Santo Toribio de Mogrovejo

para optar el grado académico de

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADA POR:

Miguel Ángel Díaz Espino

PRESIDENTE

María Arangurí García

SECRETARIO

Gregorio Manuel León Tenorio

ASESOR

DEDICATORIA

Esta tesis está dedicada a mis padres Wilder Cruz y Elena Cabrera quienes fueron los promotores de nuestros sueños y a mis hermanos por su apoyo emocional para dedicarle tiempo a seguir adelante con mis estudios de postgrado.

Dedicada a mi hija y a mí esposa M. Rosario, por robarles el tiempo que necesitaban, pero que este sacrificio sirva para demostrarles que con esfuerzo y dedicación se puede lograr todo lo que se proponen en la vida.

Nunca olviden que las amo con todo mi corazón.

AGRADECIMIENTO

A nuestro asesor Mgtr. Gregorio León Tenorio, por su apoyo en el desarrollo de este proyecto, brindándonos sus recomendaciones y experiencia profesional. Al Dr. Gilberto Carrión Barco, Dr. Ernesto Celí Arévalo, Mgtr. Oliver Vásquez Leyva, Dra. Jessie Bravo Jaico quienes me apoyaron en la evaluación, recomendaciones y validez del modelo propuesto.

Especial mención a nuestra profesora metodológica Mgtr. María Ysabel Arangurí García, cuya colaboración ha sido importante por el tiempo dedicado para las asesorías, con el fin de esquematizar este proyecto y lograr que como maestrantes pudiéramos concluir la maestría con un producto acreditable y viable para la obtención del grado de magister.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La presente tesis centra su estudio en la necesidad de incluir la gestión de riesgos de tecnologías de la información (TI) en las distribuidoras de la región Lambayeque, en el diagnóstico aplicado a una muestra de cuatro distribuidoras se detectó que estas no cuantifican sus activos de TI y el riesgo para cada uno de ellos, además no implementan una metodología de gestión de riesgos efectiva que ayuden a soportar las operaciones del negocio y evitar pérdidas económicas e imagen por riesgos materializados.

Por tal motivo, se tiene como objetivo implementar un modelo de gestión de riesgos de tecnologías de información basados en estándares adaptados en el sector de distribuidoras de la región Lambayeque para contribuir en la protección del activo de TI.

Para determinar el modelo de gestión de riesgos, se revisaron diferentes estándares y metodologías que dan soporte a la gestión de riesgos; los mismos que fueron analizados con el fin de adoptar algunas fases, procesos o actividades claves para su gestión y luego adaptarlos a la realidad del objeto de estudio.

El modelo fue validado por juicio de expertos midiendo su confiabilidad aplicando el Alfa de Cronbach y la concordancia de contenido en base a coeficiente de correlación de Kendall. Así mismo se realiza un caso de aplicación a la Empresa Distribuidora A S.A.C de la región Lambayeque. Desarrollo que sirve para el entendimiento práctico de implementación de la gestión de riesgos para cualquier tipo de empresa de nivel económico y logre contribuir a la protección de los activos de TI.

PALABRAS CLAVES: Gestión de riesgos, nivel de riesgo, tipos de riesgos, apetito de riesgo, matriz de riesgo, perfil de riesgos comerciales.

ABSTRACT

This thesis focuses its study in the necessity of including IT risk management in the distributor companies in Lambayeque region, in the diagnostic applied to a sample of four distributor companies, it was detected they do not quantify their IT assets and the risk for each one, also, they do not implement an effective risk management methodology to help to support business operations and avoid economic and image lost because of risk events.

For this reason, the objective is the implementation of a information technology risk management model based on adapted standards in the area of distributor companies in the Lambayeque region in order to contribute protecting IT assets.

To determine the risk management model, several standards and methodologies that support risk management were reviewed; and they were analyzed in order to adopt some key phases, processes or activities for the management and then fit them to the object of study.

The model was validated by expert judgment measuring its reliability by applying the Cronbach's Alpha, and the concordance level based on the Kendall correlation coefficient. Likewise, a case was implemented to the Distribuidora A S.A.C in the Lambayeque region. This development serves for the practical understanding of risk management implementation for any kind of company of certain economic level and manage to contribute to the protection of IT assets.

KEYWORDS: risk management, risk level, risk types, risk appetite, risk matrix, commercial risk profile.

INTRODUCCIÓN

En un mundo globalizado como el de hoy, la tecnología juega un papel primordial y estratégico. Esto ha generado la aparición de nuevos riesgos asociados a los sistemas que manejan la información y a la tecnología que lo soporta. La dependencia en el correcto funcionamiento de la tecnología ha aumentado el impacto sobre el negocio y sus incidentes relacionados tiene implicaciones de tipo estratégica, financiera, operacional, regulatoria, y de reputación. La gestión de riesgos no es un proceso reciente, pero a pesar de que las nuevas tecnologías han ido adquiriendo una importancia capital para el éxito de un negocio hay empresas que no han ajustado sus procesos a la toma de decisiones de TI y su gestión del riesgo; además, estas no adoptan aun estos conceptos y cultura de prevención de riesgo desde lo más alto de la organización.

En la ISO 31000:2018 se define que, "La gestión del riesgo son actividades coordinadas para dirigir y controlar la organización con relación al riesgo". [1]

Según Romeral menciona que:

> "La gestión de riesgos debe ser considerada como un proceso cíclico que incluye el análisis y la priorización de riesgos. Estas actividades permiten a la organización tener una visión detallada y exacta de los riesgos, y constituyen una buena herramienta de decisión acerca de qué riesgos pueden ser gestionados en un entorno de recursos limitados (el habitual)". [2]

La gestión del riesgo consiste en un proceso que inicia a partir de un conjunto de información que se obtiene de diferentes fuentes con el fin de obtener posibles indicadores que nos ayuden a medir el grado de cumplimiento con los objetivos de negocio y construir una organización consciente de los riesgos.

En el contexto internacional, en el ámbito de tecnología, el informe de riesgos mundiales 2018 del foro económico mundial, nos dice que:

> "Los riesgos de ciberseguridad están aumentando, tanto en su prevalencia como en su potencial desestabilizador. Los ataques contra las compañías casi se ha duplicado en cinco años y los incidentes que antes se consideraban extraordinarios son cada vez más comunes" [3].

En dicho informe se identificaron los siguientes riesgos tecnológicos:

- Ciberataques de amplio a gran escala, así como incidentes masivos de robo de información y fraudes electrónicos, los que generan aumento del costo financiero.
- Interrupción de información crítica por intrusión a infraestructura (p. ej., Internet, satélites, etc.) y de las redes.
- Explotación ilícita de información pública y privada que genera deterioro en sistemas mundiales.
- Avances tecnológicos adversos como inteligencia artificial, geoingeniería y biología sintética que pueden provocar desastres ambientales, económicos y humanos. [3, p.3]

Los resultados del informe indican que los ciberataques ocupan el tercer lugar de top 10 riesgos en término de probabilidad y el puesto seis en cuanto a impacto: mientras que el fraude o robo de datos ocupa el cuarto puesto de probabilidad [3, p.3].

Según Deloitte manifiesta: "El pasado mayo 2017 se produjo un ciberataque que afectó a más de 360.000 dispositivos electrónicos de más de 180 países, bloqueándolos e impidiendo su utilización" [4]. Por lo cual, el mismo autor agrega que: "…. se estima que el impacto económico podría superar los 200 millones de dólares, sin lugar a duda ha sido uno de los mayores ciberincidentes de los que se tiene constancia" [4, p. 32].

Por su parte, la revista ComputerWorld nos dice que: "La pérdida o alteración de la información asociada a fallos de seguridad, puede representar un alto coste para las organizaciones, además de la pérdida de oportunidades de negocio y una posible mala reputación de la marca" [5]. Basta echar un vistazo a hechos que dejamos atrás como hackeo a Yahoo donde más de mil millones de cuentas afectadas, el ciberataque a España que afectó a Telefónica y Equifax donde robaron información de 143 millones de usuarios [5, p. 95].

Según Deloitte, "Las Organizaciones en Latinoamérica se encuentran inmersas en un contexto de fuerte desarrollo de negocios digitales y de mayor exposición a las ciberamenazas inherentes a este nuevo contexto de negocios" [6]. En los resultados obtenidos revelan que cuatro de cada diez organizaciones sufrieron una brecha de seguridad en los últimos veinticuatro meses y menos del 10% de las organizaciones

cuentan con un tablero con indicadores (KPI) que permite evaluar la gestión de cyber riesgos y de seguridad de la información. Los ejecutivos responsables de administrar la seguridad de la información consideran que aún no cuentan con recursos suficientes y son conscientes que tienen un largo camino por recorrer. [6, p. 10].

Así mismo, el estudio realizado por PricewaterhouseCoopers dice que: Los cambios regulatorios "sobre-regulación" son las razones de que haya una mayor percepción de riesgo y algunos supervisores están siendo mucho más rigurosos y menos flexibles en cuanto al cumplimiento de las normas, además los consumidores también son más exigentes, es decir están evolucionando su forma de querer comprar o recibir un servicio [7].

En el contexto nacional, EY (antes Ernst & Young) lanzó la encuesta "Gobierno, riesgo y cumplimiento 2015" (de ahora en adelante se denomina, encuesta GRC 2015), afirma que:

> "En el Perú sólo el 33% de los encuestados hace uso de una o más tecnología GRC. Asimismo, la encuesta muestra que el 58% de las empresas peruanas no cuenta con una gerencia de riesgos, mientras que del 42% restante, solo un 9% reporta funcionalmente sus riesgos al directorio o en alguno de sus comités". [8].

Por otro lado, un reciente estudio de Forbes menciona que, para el 2019 la ola del cibercrimen en el mundo alcanzará los US$ 2.1 billones y el Perú se encuentra en el séptimo lugar de Latinoamérica afectados por el cibercrimen, registrando pérdidas económicas por ciberataques que ascendieron a USD 4,782 millones, en esa línea, los sectores que se han visto más afectados por ciberataques han sido el negocio retail, el sector salud y el sector construcción. Según el foro económico mundial (WEF), gran parte de estas pérdidas pasan sin ser detectadas, especialmente las originadas por el espionaje industrial. Los temas que siguen sin estar completamente monitoreados según la WEF son información sobre infraestructura nacional y recursos naturales, propiedad intelectual, información confidencial y estratégica, fraudes, mercado negro cyber, todo tipo de estafa online, así como otro delitos informáticos.

En el contexto de la organización, la investigación se realizará a empresas distribuidoras de la región Lambayeque dedicada a venta y distribución de artículos de ferretería, acabados y materiales de construcción (Caso de Estudio: Distribuidora Local). La distribuidora, inició sus operaciones en el año 1993 en el norte del país. Actualmente, cuenta con diecisiete tiendas comerciales a nivel nacional con sede central de sus operaciones administrativas en la ciudad de Chiclayo y tiene como objetivo corporativo: la expansión del mercado y mejorar la calidad de servicio al cliente. Sus principales procesos críticos son: gestión de compras, ventas, contable y financiera; los cuales se encuentran soportados por un sistema de información desarrollado por un tercero. El área de T.I está centralizada y orienta sus actividades en brindar soporte de desarrollo y mantenimiento de las aplicaciones empresariales, así como otros servicios informáticos a las diferentes áreas de todas sus sedes a nivel nacional. El área de TI está ubicada organizacionalmente dentro de la Gerencia de Administración y Finanzas.

En el ejercicio operativo de la empresa el volumen de procesamiento de datos ha empezado aumentar considerablemente teniendo un resultado en la determinación eficiente de su infraestructura tecnológica. En su infraestructura la organización cuenta con servidores y comunicaciones limitados, un servidor de base de datos de producción y cuatro servidores para conexión de red: dos comparten el sistema de información cliente-servidor que corren con el servicio terminal server (protocolo RDP) y active directory, un servidor de aplicaciones web y un servidor instalado Linux Centos que cumple la función de establecer conexión VPN (OpenVPN) a nivel nacional y de firewall básico perimetral; también, la empresa tiene un parque de 240 PC's las cuales el 38% son de tecnología celeron a dual core. La consecuencia que ha ocasionado, que los procesamientos y consulta de información de periodos largos se limiten a determinado horario de trabajo porque afecta en lentitud las operaciones. La frecuencia de ocurrencia es los meses de mayor tráfico como enero, julio y diciembre. Si bien es cierto que las operaciones siguen su curso debe garantizarse la continuidad de los servicios y soportar tecnológicamente el crecimiento de la organización.

Cabe mencionar que, otro de los riesgos presentes es, en cuanto a infraestructura física por su edificación, la división del área de sistemas con el centro de datos es a través de paredes de material de Drywall, ventana de vidrio y puertas contraplacadas de cartón prensado, la distribución de energía del área está por medio de un subtablero para todo el piso que se comparte con los equipos de aire acondicionado, el ambiente de servidores carece de estabilización y generador de energía, en el área se provee de detectores de humo ubicados al centro del ambiente y fuera del centro de datos, también se cuenta con un extintor manual de fuego. La deficiente distribución de energía y capacidad de autonomía eléctrica ha ocasionado la interrupción del servicio del centro de datos de cinco veces en los dos últimos años por un lapso de una a cuatro horas. La consecuencia a nivel económico ha sido aproximadamente de S/198,000 ocasionado por interrumpir las operaciones comerciales a nivel nacional que impacta al crecimiento de las ventas. Aunque la empresa ha crecido en los últimos años el software principal que soporta todos los procesos del negocio tiene una antigüedad aproximada de quince años y fue desarrollada para entornos Windows. El lenguaje utilizado de origen para el desarrollo del sistema fue FoxPro7; luego, se actualizó a su versión FoxPro9 y base de datos SQL Server 2008, esto ha ocasionado una limitada compatibilidad con versiones de sistemas operativos, integración con nuevos sistemas y portabilidad a dispositivos móviles, condiciones que limitan la escalabilidad funcional y su soporte. La empresa ha direccionado su esfuerzo a fabricar su propio software, con tecnología web que sea compatible con el sistema de gestión comercial principal, hecho que generó pérdidas económicas de S/252,200 por motivo que el entregable del proyecto no cumplió con las expectativas de la organización.

Los backup de base datos se realizan por las noches con frecuencia diaria una sola vez al día y es almacenada de manera comprimida en discos externos en el mismo centro de datos; asimismo, se tiene como práctica que los backup son restaurados una vez al año cuando se realiza cierre de inventario o recuperar alguna información eliminada accidentalmente por el administrador de base de datos, motivo que afecta a detectar fallos de restauración y recuperación.

La información de la empresa, es almacenada en los equipos del usuario dueño del proceso, sin respaldo alguno por confidencialidad de la misma, medida que ha originado pérdidas de la información, por daños físicos de hardware de disco duro en el equipo, dicho incidente ha ocurrido tres veces en los tres últimos años. El impacto ocasionó retrasos en los procesos operativos de atención al cliente interno y externo además de información relevante que asciende en términos económicos de S/5,250.

Se ha tenido tres ataques informáticos en los tres últimos años, el primer ataque ocurrió en el 2016 fue un ataque de phishing que atentaba con las transacciones bancarias que se generan por compras en el exterior del país, el segundo en el 2017 fue un ataque de denegación de servicios en el router de telefónica, el tercero sucedió en el 2018 fue un ataque Ransonware WannaCry contra un servidor de conexión remota de usuarios. Para el primer incidente el proveedor del hosting de correo en conjunto con el área de sistema aplicó filtro de contenido de spam; para el segundo caso, se aplicaron controles de acceso y conexión al router por parte del proveedor de servicio de internet. En el tercer caso, se realizó la actualización de los sistemas operativos a Windows 7, instalación de antivirus y antimalware con licencia free. Las consecuencias de los ataques fueron la realización de transferencias bancarias a suplantadores de identidad, pérdida de información y puso en riesgo la continuidad del servicio.

Debido al crecimiento experimentado en los cinco últimos años, la empresa cuenta con un número inadecuado de licencias de software de uso comercial, lo cual conlleva a problemas legales de propiedad intelectual, además del no acceso a actualizaciones de seguridad de software. En el año 2016 se recibió una carta del departamento de licencias de Microsoft Perú con el fin de sustentar las licencias adquiridas por la empresa. El cual incurrió en adquirir determinadas licencias que evitarán sanciones económicas y administrativas.

En la sucursal de Chiclayo se cuenta con seis tiendas conectadas localmente a la sede central de operaciones administrativas y sistemas. Estos locales comerciales se encuentran en el mismo segmento de red conectado a través de radio enlaces con torres de altura entre nueve a dieciocho metros. La conexión al mismo segmento concreta un déficit de rendimiento de red, aprovechamiento del ancho de banda, seguridad y confidencialidad

de la información. En el primer trimestre del periodo 2018 se presentó un incidente que ocasionó el colapso de la red LAN por la conexión de un switches que generó bucles de broadcast.

El personal de soporte técnico, tiene acceso a través de herramientas de acceso remoto a monitorear y dar asistencia a todos los equipos de la empresa; así como, acceso a los servidores de red nivel administrador para crear usuarios remotos o realizar acciones durante un incidente. La conexión remota directa con el fin de facilitar soporte de equipos ha generado suspicacia con algunos usuarios de nivel jefaturas y gerentes por la posibilidad de un acceso no autorizado a los equipos.

Las solicitudes para crear, dar de baja, establecer los niveles de acceso a los usuarios en el sistema de información y otros servicios de informática como correo y acceso a internet son autorizadas por la jefatura de cada área y es enviada a la jefatura de sistemas quien designa al área de soporte técnico la creación del perfil y asignación de accesos al usuario. Medio que no provee las garantías necesarias para la seguridad y confidencialidad de la información.

El diagnóstico interno permitió identificar que la organización no aplica procesos estandarizados y controles que permitan afirmar la seguridad de los equipos y de la información sustentada en políticas de seguridad y mejores prácticas que garanticen la continuidad de los servicios.

En conclusión, los directivos omiten y no son reflexivos del riesgo e impacto que las amenazas expuestas generan y las pérdidas que pueden ocasionar si no son controladas a tiempo y de forma adecuada. Para ello, la presente investigación busca aplicar estándares y metodologías para la gestión de los riesgos tecnológicos cuya finalidad es la protección de la información, los activos de alto valor y definir el tiempo objetivo de recuperación (en adelante RTO, por sus siglas en inglés) aceptable para el negocio.

Por lo antes mencionado, esta investigación se formula la siguiente interrogante ¿De qué manera se podrá contribuir en la protección del activo de TI en el sector de distribuidoras de la región Lambayeque? Para proponer una alternativa de solución para la adecuada gestión de riesgo en el sector de estudio, se plantearía la siguiente respuesta con la

implementación de un modelo de gestión de riesgos de TI basado en estándares adaptados se logra contribuir en la protección del activo de TI en el sector de distribuidoras de la región Lambayeque.

El presente trabajo de investigación tiene como propósito implementar el modelo de gestión de riesgos de tecnologías de información basados en estándares adaptados en el sector de distribuidoras de la región Lambayeque para contribuir en la protección del activo de TI y como objetivos específicos los siguientes puntos:

a) Armonizar estándares, metodologías y herramientas para el análisis y gestión de riesgos de TI, con la finalidad de determinar el modelo.
b) Proponer el modelo de gestión de riesgos adaptado para identificar y abordar los factores de riesgos que afectan el activo de TI en el contexto del sector de distribuidoras.
c) Implementar el modelo de gestión de riesgos de TI para contribuir en la protección del activo de TI en un caso de estudio.
d) Validar el modelo de gestión de riesgos mediante juicio de expertos, para valorar el modelo adaptado.

Para justificar la importancia de esta investigación se plantea en este proyecto las siguientes razones:

En lo tecnológico, este proyecto propone un modelo de gestión de riesgos de TI como una alternativa de solución a las organizaciones para contribuir en la protección del activo de TI de las amenazas expuestas con el fin potenciar la capacidad de respuesta inmediata en la continuidad del servicio brindado. La investigación busca aplicar estándares y metodologías para apoyar la toma de decisiones efectiva en la gestión de riesgos bien informados y justificar los gastos que forman parte de un presupuesto de TI.

Desde el punto de vista económico, la utilización de la gestión de riesgos en TI puede evitar pérdidas económicas, activos relevantes para la empresa y protección de la marca.

En lo científico, si bien hoy en día existen estándares e incluso metodologías para gestionar riesgos es importante mencionar que muchos de estos plantean una amplia variedad de escenarios de los cuales no centra la importancia en gestionar los riesgos que afectan directamente a los objetivos del negocio y sus activos tecnológicos que soportan su operación, motivo por el cual se consideró importante desarrollar un modelo de gestión de riesgos que adecuado a la realidad de este sector permite elevar su nivel de resilencia y disminuir pérdidas económicas generadas por la materialización de riesgos, los mismos que puedan conllevar a la paralización de las actividades del negocio.

Con respecto a lo social, la evaluación de los riesgos de tecnologías de la información le permitirá a la organización brindar información a los miembros de la alta dirección para desarrollar una efectiva gestión de riesgos y aplicar controles que permitan adquirir y mantener servicios informáticos más eficientes además de mejorar la atención y experiencia de compra de los clientes. Así también, se pretende dar mayor realce a la gestión de riesgo en empresas del mismo sector de la región Lambayeque, mediante el aporte del conocimiento adquirido en el presente estudio.

CAPÍTULO I. MARCO TEÓRICO CONCEPTUAL

1.1 Antecedentes

Según Cristhian [9], en su investigación nos dice que en Ecuador las empresas se encuentran expuestas a ataques informáticos en los sistemas que manejan dentro de sus organizaciones y de problemas asociados al uso de los recursos físicos. De acuerdo a una auditoría previamente realizada en las empresas se identificaron los siguientes riesgos en el departamento de TIC: Errores en el sistema utilizado, asociados principalmente a la corrupción de los datos; la exposición a malware, que afecta el correcto funcionamiento de los equipos informáticos; la propagación de virus entre ordenadores, atribuido a la descarga de información o apertura de correos maliciosos; el procesamiento de datos incorrectos, eliminación de datos descuidados, o la apertura accidental de archivos adjuntos de correos electrónicos infectados; y amenazas informáticas relacionadas con el robo de información confidencial. Como resultado se obtuvo que las normas ISO 9001, 27005 y 31000 presentaron características adaptables y aplicables a un modelo integrado de gestión de riesgos, que se ajusta a los requerimientos de las TIC, así como los procesos y activos de la información relacionados con ellas; adicionalmente, se aplicó el modelo a la Fiscalía General de El Oro con la finalidad de validar el mismo. La tesis toma como base este antecedente ya que se analizaron las normas que constituyen fuentes para el desarrollo de un modelo de gestión de riesgos y aspectos más relevantes en cuanto a procesos aplicable a cualquier organización pública o privada.

Según M. Arangurí, R. Imán y G. León [10], en su investigación nos dice que en el contexto de universidades de la región Lambayeque, no se ha dimensionado la necesidad de una efectiva gestión de riesgos, por desconocimiento, complejidad y aplicación, se cita que no existe un modelo aplicado al contexto universitario que ofrezca características de simplicidad y flexibilidad. Para la obtención de los resultados se identificaron fases coincidentes en cada estándar y metodologías de gestión de riesgos las cuales fueron adaptadas y tomadas a la estructura base de la ISO 31000:2009. Para su aplicación, definieron características de practicidad (clasificación, dependencias y valoración de activos y el impacto en los procesos del negocio), flexibilidad (líneas base de adaptación a la realidad del contexto universitario y su aplicación en cada fase) y

confiabilidad (valorada por juicio de expertos). Del análisis de los resultados se desprende que se mejora el nivel porcentual de actitud proactiva para la gestión de riesgos en un valor promedio de 75%. La relación con la presente investigación es referente al análisis de estándares y metodologías valoradas por juicios de expertos, la adaptación de un modelo de referencia para la evaluación de riesgos de tecnologías de información y el impacto en los procesos del negocio para apoyar a una gestión efectiva de los riesgos.

La tesis de E.Chillogallo y V. Zambrano [11], se centra en una institución del estado con más de 180 puntos a nivel nacional y que tiene como misión dirigir con objetividad y ética la investigación del delito. En el contexto de su realidad, nos dice que existe escasa realización de evaluaciones de los riesgos de TI en la institución; además, que no se tiene identificado el número de activos afectados en caso de la aparición de un evento de riesgo. En los resultados de la investigación se indica que las metodologías y normas valoradas por la Contraloría General del Estado y el Esquema Gubernamental de Seguridad de la Información son NTE INEN-ISO-31000, NTE INEN-ISO/IEC 27005. Como conclusiones, se obtuvieron que el modelo tiene una aplicación práctica, pero requiere de un proyecto con recursos y tiempos definidos. Los modelos de gestión de riesgos actuales cumplen adecuadamente con las etapas básicas de gestión, pero se debe en lo posible adecuar las características de estos modelos para que sean personalizados a la realidad institucional. La relación con la presente investigación es la creación de un modelo definido de estándares que la organizaciones valoran para la gestión de riesgos de tecnologías de la información como ISO: 31000 y 27005, normas que permiten su aplicabilidad al 100%, el desarrollo de planes y estrategias sostenibles de gestión de riesgos, pero requieren trabajo de personalización para ser empleada a la realidad de la organización.

Según M. Fernanda [12] la información durante mucho tiempo ha sido considerada como un activo valioso e importante, el aumento de la economía del conocimiento ha llevado a las organizaciones a depender cada vez más en la información y sobre todo de TI. Diferentes eventos o incidentes pueden causar impactos adversos en los procesos de negocio de la organización y de su misión, que van desde intrascendente a catastrófica.

El resultado permitió identificar el nivel de riesgo en que se encuentran los activos de la organización; además, del nivel de madurez de la seguridad implementada. Como conclusiones, se indica MAGERIT es una metodología que permite conocer las amenazas a los cuales están expuestos la organización para finalmente sugerir las salvaguardas necesarias para reducir los niveles de riesgo e impacto; asimismo, el plan propuesto sirvió para incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos de tecnología de información. La herramienta PILAR permitió ingresar las valoraciones para realizar las evaluaciones referentes a los activos y amenazas para finalmente obtener los niveles de riesgo e impacto plasmados en gráficas radiales. La relación con la presente investigación es que Margerit es la metodología más utilizada para desarrollo de análisis de riesgos e identificación de activos de tecnologías de información y PILAR es una herramienta complementaria que permitirá graficar los niveles de riesgos e impacto que la empresa debe considerar para la aplicación de controles.

En su publicación G. Vanegas y C. Pardo [13], nos dice que actualmente las grandes organizaciones dependen del uso de la tecnología donde la información es un activo vital para ser exitosas y lograr su continuidad en el mercado. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. El estudio plantea una propuesta metodológica que surge del estudio realizado a cada uno de los modelos y estándares relacionados con la gestión de riesgos en TI, la cual está basada en la combinación de las actividades descritas en los procesos de gestión de riesgos de cada uno de los modelos; esta propuesta permitirá a las empresas desarrolladoras de software u organizaciones que tengan procesos en TI, lograr identificar, analizar y dar seguimiento a los riesgos en sus proyectos en desarrollo. En las conclusiones se indica que el análisis realizado permitió evidenciar que la mayoría de las normas y modelos aquí descritas están relacionados entre sí, aunque algunas normas presentan procesos más detallados, con un nivel más profundo que otros modelos. En la elaboración de este artículo, se relaciona con la investigación por la mención de los modelos de gestión del riesgo existentes desde su evolución los cuales serán estudiados para poder ser adaptados a la organización.

D. Moncayo [14], hace una evaluación del contexto de las pequeñas y medianas empresas, reconociendo que no se conocen de forma clara los riesgos a la que está sometida su organización, parte de ellas aplican planes de contingencia a nivel empresarial, pero no cuantifican sus activos y el riesgo por cada uno de ellos. Por ese motivo, este antecedente propuso la creación de un modelo de evaluación de riesgos, basado en las metodologías Magerit, Octave y normas NIIF (Normas Internacionales de Información Financiera), el mismo que aportó a las empresas a obtener información sobre los riesgos, amenazas, y protecciones que se deben considerar para evitar y tomar medidas de prevención oportuna y adecuada. En la elaboración de este artículo se muestra estándares y normas que se debe considerar al realizar un análisis de riesgos. Posteriormente, se muestra y explica cómo utilizar una norma y metodología desde un perfil más básico para PYMES y desarrollar en forma exitosa este tipo de iniciativas.

1.2 Base Teórico-Conceptual

Para dar soporte a esta investigación, se ha considerado pertinente definir algunos marcos de gobierno y de gestión, normas y metodologías que se debe considerar para la gestión de riesgo.

COBIT 5, provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

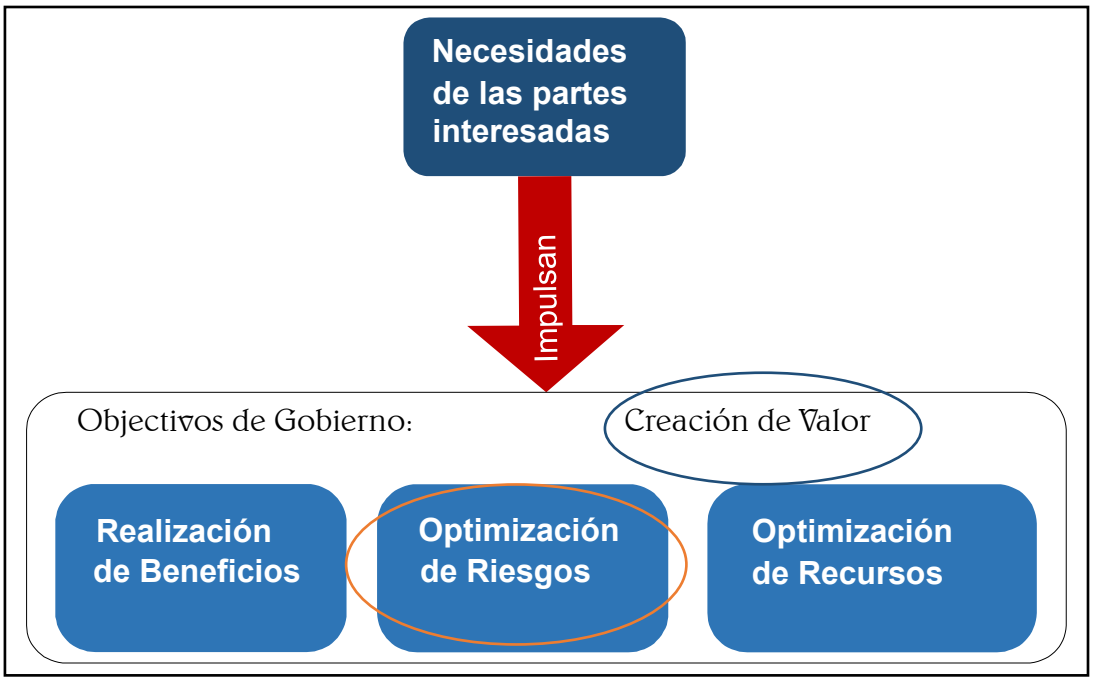
COBIT 5 permite que las tecnologías de la información se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas. [15]

COBIT 5, es pertinente para la investigación debido que uno de los objetivos de gobierno requiere reconocer los riesgos para aportar a la generación del valor; además, presenta un modelo integral, estructurado y lógico de mejores prácticas de

Tecnología de Información para evaluar y/o auditar la gestión y control de los sistemas de información y tecnología, este marco es potencial para las organizaciones, porque fue definido por un consenso de expertos en todo el mundo en aspectos técnicos, seguridad, riesgos, calidad y control.

La estructura propone un marco de acción donde se evalúen los requerimientos del negocio, los recursos de TI y a los procesos de TI; los cuales pueden ser enfocados desde las metas corporativas y metas de TI como por ejemplo: la calidad y seguridad del servicio, generar valor al negocio con las inversiones en TI para alcanzar metas estratégicas, conseguir beneficios a través del uso eficiente de la tecnología y, finalmente, realizar una evaluación sobre los procesos del negocio más relevantes que son soportados por TI y que apoyan a las metas de la organización.

Figura 1: El Objetivo de Gobierno: Creación de Valor

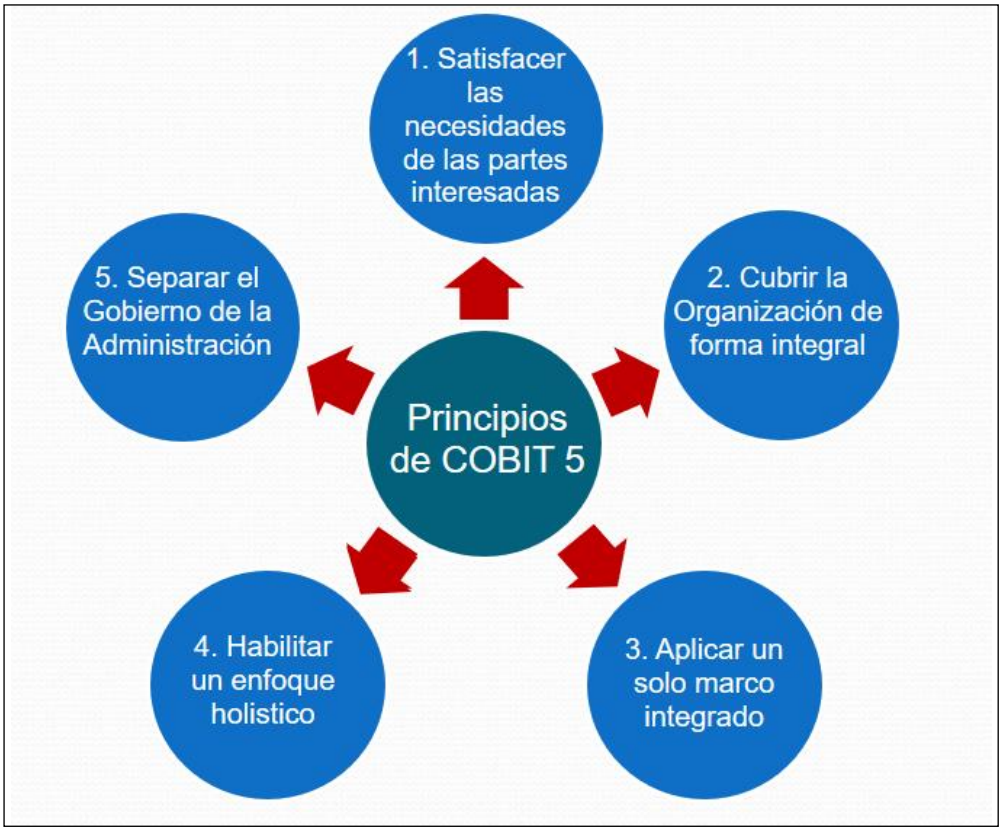


Fuente: ISACA. "COBIT® 5: Un Marco de Negocio para el Gobierno y la Gestión de la Empresa", U.S, abril, 2012.

Principios de COBIT 5

COBIT 5 une cinco principios que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie holística de siete habilitadores, que optimizan la inversión en tecnología e información, así como su uso en beneficio de las partes interesadas.

Figura 2: Principios de COBIT 5



Fuente: ISACA. "COBIT® 5: Un Marco de Negocio para el Gobierno y la Gestión de la Empresa", U.S, abril, 2012.

a) **Satisfacer las partes interesadas:** Las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de Gobierno. La cascada de metas de COBIT 5 traducen las necesidades de las Partes Interesadas en metas específicas, accionables y personalizadas dentro del contexto de la Organización, de las metas relacionadas con la TI y de las metas habilitadoras.

Figura 3: Visión General de la Cascada de Metas de COBIT 5

Fuente: ISACA. "COBIT® 5: Un Marco de Negocio para el Gobierno y la Gestión de la Empresa", U.S, abril, 2012.

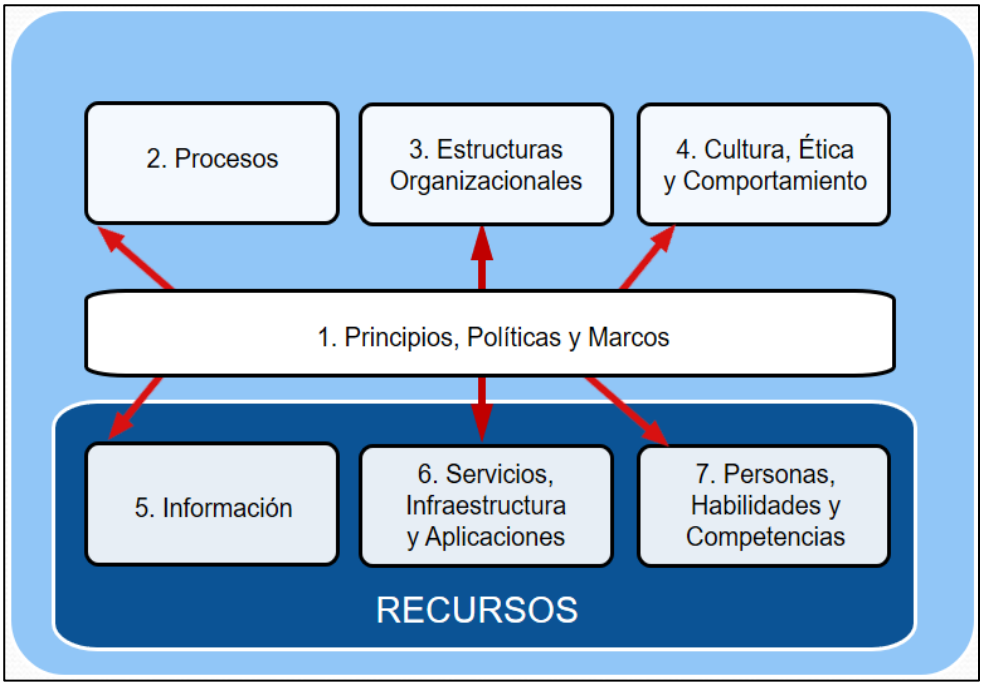
b) **Cubrir la Compañía de Forma Integral:** Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo amplio, COBIT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos.

c) **Aplicar un marco de referencia único integrado:** COBIT 5 se alinea con otros estándares y marcos de referencia relevantes usados por las organizaciones y, por tanto, permite a la empresa usar COBIT 5 como el marco integrador general de gestión y gobierno de TI.

d) **Hacer posible un enfoque holístico:** Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa.

COBIT 5 describe 07 categorías de habilitadores y se muestran en la siguiente imagen.

Figura 4: Catalizadores Corporativos COBIT 5



Fuente: ISACA. "COBIT® 5: Un Marco de Negocio para el Gobierno y la Gestión de la Empresa", U.S, abril, 2012.

e) **Separar el gobierno de la gestión:** COBIT 5 efectúa una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos.

La posición de COBIT 5 sobre esta fundamental distinción entre gobierno y gestión es:

- **Gobierno**

  El gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

- **Gestión**

  La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

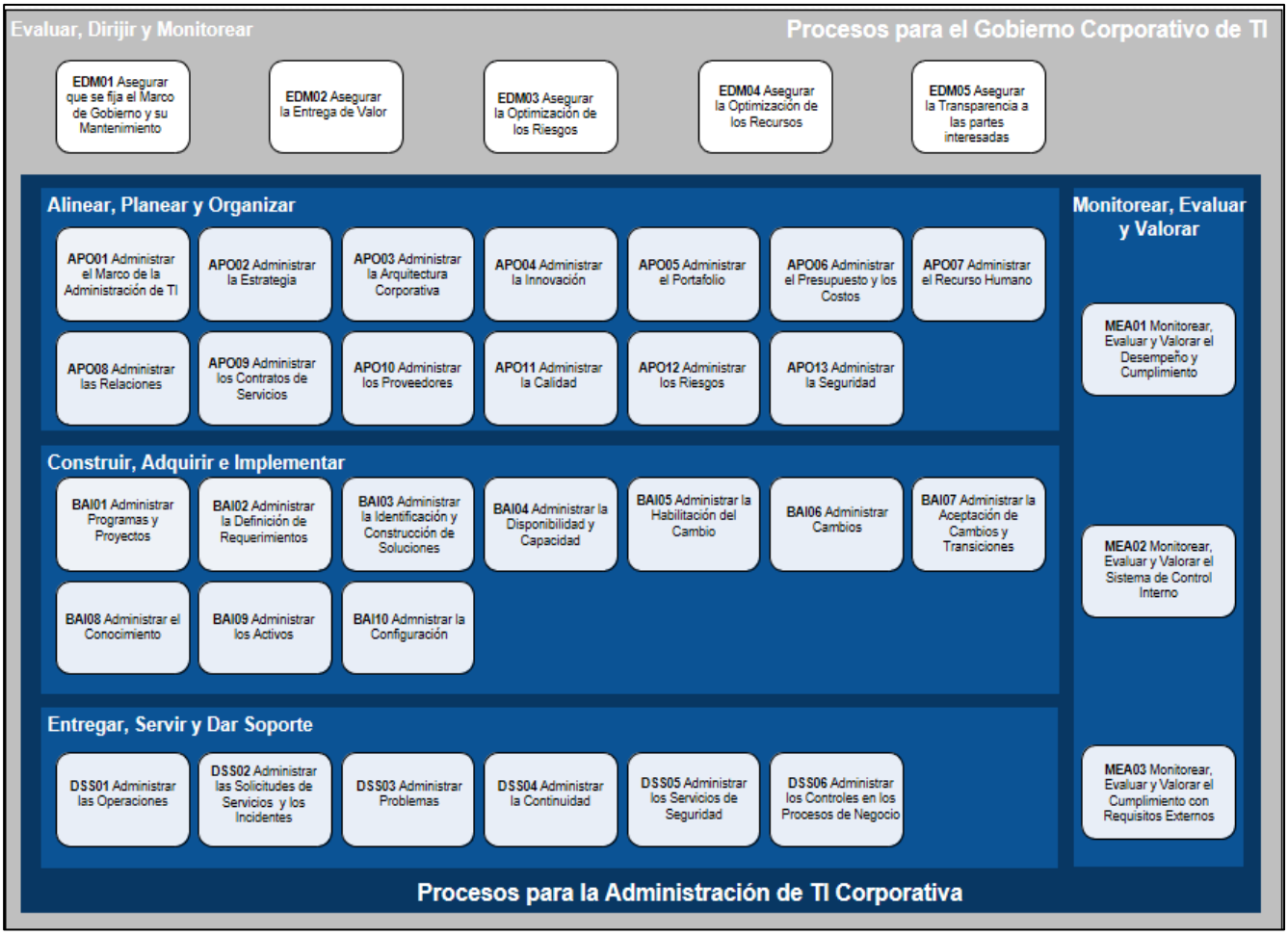
Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

Procesos Habilitadores

COBIT 5 incluye un modelo de referencia que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente encontramos en una empresa relacionados con las actividades de TI, proporciona un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio. El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

La incorporación de un modelo operacional y un lenguaje común para todas las partes de la empresa involucradas en las actividades de TI, es uno de los pasos más importantes y críticos hacia el buen gobierno. Adicionalmente proporciona un marco para medir y vigilar el rendimiento de TI, proporcionar garantía de TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión. [9, pp. 13 - 33]

Figura 5: Modelo de Referencia de Procesos de COBIT 5



Fuente: ISACA. "COBIT® 5: Un Marco de Negocio para el Gobierno y la Gestión de la Empresa", U.S, abril, 2012.

Estándares de Gestión del Riesgo

ISO 31000: 2018

Esta norma es importante para la gestión del riesgo porque recoge una serie de buenas prácticas internacionales que proporcionan sólidos principios y directrices para la gestión eficaz del riesgo a nivel operativo y de gobierno. Las directrices, fases y su modelo estructurado son pertinentes para el desarrollo del modelo de riesgos de la investigación puesto que permite adaptarse a cualquier sector económico y a su contexto, así mismo las organizaciones que la utilizan pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido a nivel internacional y crear un alto nivel de confianza para las partes interesadas, es preciso mencionar que esta norma no está prevista para fines de certificación.

Para la ISO 31000, el propósito de la gestión del riesgo es la creación y la protección del valor. La cual permite mejorar el desempeño, fomenta la innovación y contribuye al logro de objetivos. El desarrollo de su marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la organización. Es una norma práctica que pretende ayudar a las organizaciones en el desarrollo de su propio enfoque de la gestión del riesgo, estableciendo los principios racionales para la ordenación eficaz.

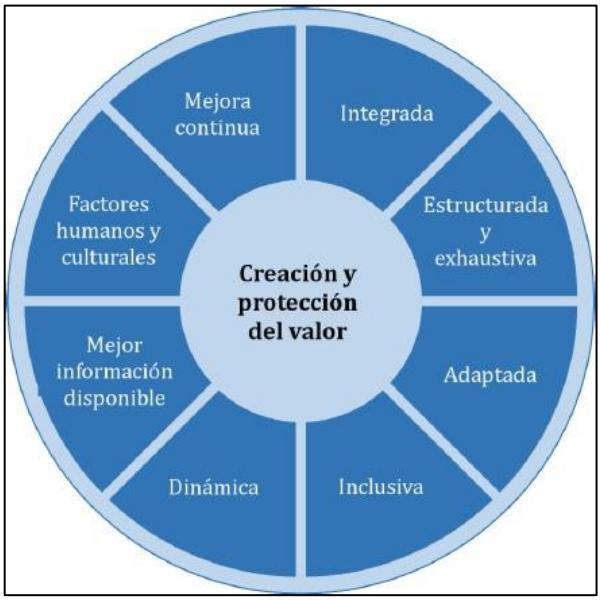
Principios

Para que la gestión de riesgos sea eficaz, una organización debe contar con los siguientes principios (ISO 31000, 2018):

a) Integrada: La gestión del riesgo es parte integral de todas las actividades de la organización.
b) Estructurada y exhaustiva: Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.
c) Adaptada: El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.

d) Inclusiva: La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.
e) Dinámica: Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
f) Mejor información disponible: Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
g) Factores humanos y culturales: El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
h) Mejora continua: La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

Figura 6: Principios



Fuente: ISO 31000:2018(es) "Risk management— Guidelines," USA. 2018

Marco de Referencia ISO 31000:2018

El propósito del marco de referencia de la gestión del riesgo es asistir a la organización en integrar la gestión del riesgo en todas sus actividades y funciones significativas. La eficacia de la gestión del riesgo dependerá de su integración en la gobernanza de la organización, incluyendo la toma de decisiones. Esto requiere el apoyo de las partes interesadas, particularmente de la alta dirección.

El desarrollo del marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la organización

Figura 7: Marco de Referencia

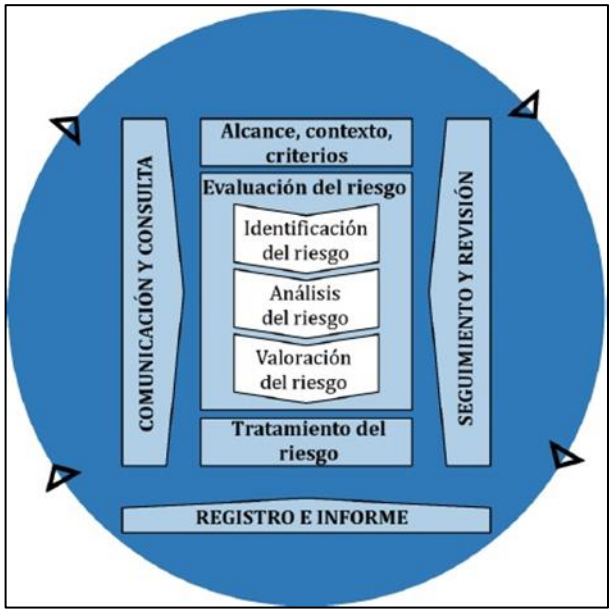
Fuente: ISO 31000:2018(es) "Risk management— Guidelines," USA. 2018

La organización debería valorar sus prácticas y procesos existentes de la gestión del riesgo, valorar cualquier brecha y abordar estas brechas en el marco de referencia. Los componentes del marco de referencia y la manera en la que trabajan juntos, deberían adaptarse a las necesidades de la organización.

Procesos de la Gestión de Riesgos ISO 31000:2018

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. [1, p. 10-21]

Figura 8: Procesos



Fuente: ISO 31000:2018(es) "Risk management— Guidelines," USA. 2018

ISO 27005

Esta norma proporciona directrices para la gestión de riesgos de seguridad de la información y nos interesa en la investigación para no tener dudas sobre los diferentes elementos que debe incluir toda metodología de análisis de riesgos.

La norma ISO 27005 no proporciona la metodología concreta para el análisis de riesgos, sino que describe en forma de cláusulas el proceso que se recomienda seguir para analizar el riesgo en las organizaciones. La norma incluye 6 anexos diferentes que van desde la A hasta la F que son de carácter informativo y no normativo, presenta orientación para realizar la identificación de activos e impactos, ciertos ejemplos de vulnerabilidad y las amenazas que se pueden asociar, hasta diferentes aproximaciones

para realizar el análisis que distingue entre análisis de riesgos de alto nivel y análisis detallado. Además es compatible con los conceptos generales especificados en la norma ISO/ IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de elementos que permitan garantizar la seguridad de la información basada en un enfoque de gestión de riesgos. La norma es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que podrían comprometer la seguridad de su información (ISO/IEC, 2011a). [16]

BS 31100

La BS 31100: 2011, es un estándar británico que ha sido referenciada porqué proporciona recomendaciones prácticas y específicas sobre cómo implementar los principios clave de una gestión de riesgos efectiva. La BS 31100 se basa en la mejor información disponible y actualizada sobre el desarrollo, implementación y mantenimiento de una gestión de riesgos proporcional y efectiva alineada con ISO 31000, además su aporte teórico-práctico nos permite entender el proceso de implementación de las fases de la ISO 31000. [17]

COSO ERM

COSO II o COSO ERM, proporciona un marco para la gestión de riesgos empresariales integrados con la estrategia y desempeño, que generalmente implica la identificación de eventos o circunstancias particulares pertinentes a los objetivos de las organizaciones (riesgos y oportunidades), la evaluación en términos de probabilidad y magnitud del impacto, que determina una estrategia de respuesta, y el monitoreo del progreso.

COSO ERM, es pertinente para la investigación porqué proporciona una mayor comprensión del valor de la gestión de riesgos en un entorno empresarial. [18]

Metodologías

Las metodologías de gestión de riesgos de TI, establecen una estructura de trabajo para desarrollar un orden secuencial y formal que permita establecer resultados

coherentes para en cada contexto particular definir las necesidades diagnosticadas, establecer las estrategias preventivas y asegurando la efectiva generación de valor de las tecnologías de información.

MAGERIT

Es un método formal para investigar los riesgos derivados del uso de la tecnología de información y las comunicaciones. Es una norma establecida por el Gobierno Español con el fin de brindar una metodología de análisis y gestión de riesgos caracterizado en los activos de TI. El propósito de MAGERIT está relacionado con el valor que representan los activos de TI para la organización así como las dependencias entre los diferentes activos informáticos y tecnológicos, los mismos que inmersos a ciertos riesgos se deben minimizar con medidas de seguridad, para mitigar la desconfianza en el uso de estos. Su utilización está enfocada en las personas que utilizan los sistemas de información y sobre los riesgos y vulnerabilidades a que está expuesta la información (MHAP, 2012). [19]

Margerit es conveniente para esta investigación porqué incluye como activos de TI: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos, los cuales son activos necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

OCTAVE

Es una técnica efectiva de evaluación de riesgos desarrollada en el Centro de Coordinación CERT en *Carnegie Mellon University*. Octave, es pertinente para la investigación porqué aporta un conjunto de conceptos, herramientas, técnicas y métodos para la evaluación del riesgo en activos de TI. Tiene en cuenta también la definición de los activos incluyendo: personas, hardware, software, información y sistemas como Margerit. Su metodología original que conforma la base de su conocimiento tiene tres componentes principales descritas como vista organizacional, vista tecnológica, estrategia y plan de desarrollo, las mismas que en su núcleo

describen conjuntos de criterios (principios, atributos y resultados); Octave, proporciona una línea base que se puede utilizar para enfocar la mitigación y mejorar la toma de decisiones con base en riesgos en tres pilares relacionados su confidencialidad, integridad y disponibilidad (CERT, 2008). [20]

CRAMM

Es la metodología de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico. El significado del acrónimo proviene de CCTA Risk Analysis and Management Method. Su versión inicial data de 1987 y la versión vigente es la 5.2. Al igual que MAGERIT, tiene un alto calado en administración pública británica, pero también en empresas e instituciones de gran tamaño. Dispone de un amplio reconocimiento. La metodología de CRAMM incluye las siguientes 3 etapas:

La primera de las etapas recoge la definición global de los objetivos de seguridad entre los que se encuentra la definición del alcance, la identificación y evaluación de los activos físicos y software implicados, la determinación del valor de los datos en cuanto a impacto en el negocio y la identificación.

En la segunda etapa de la metodología se hace el análisis de riesgos, identificando las amenazas que afecta al sistema, así como las vulnerabilidades que explotan dichas amenazas y por último el cálculo de los riesgos de materialización de las mismas.

En la tercera etapa se identifican y seleccionan las medidas de seguridad aplicadas en la entidad obteniendo los riesgos residuales, CRAMM proporciona una librería unas 3000 medidas de seguridad. [21]

CRAMM, es referenciada para la investigación porqué es una metodología similar a Margerit que permiten identificar riesgos y amenazas que podrían afectar en integridad, confidencialidad y disponibilidad de los activos de TI.

RISK IT

Es un marco de trabajo a nivel mundial enfocado a las TI y publicado por ISACA. RISK IT proporciona una visión global sobre los riesgos empresariales asociados con todas las actividades relacionadas con TI.

RISK IT pretende ser una herramienta práctica para la gestión de riesgos basada en los conceptos de valor y beneficios que la organización obtiene a través de sus iniciativas de TI. Al igual que COBIT, RISK IT se concentra en el cumplimiento de los objetivos de la organización. Este modelo puede personalizarse para cualquier tipo de empresa en cualquier ubicación geográfica. RISK IT se define como una serie de guías para la gestión eficaz de los riesgos de TI. Dichas guías se basan en los principios comúnmente aceptados en ERM, que se han aplicado en el ámbito de las TI. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones puedan poner los principios en práctica y comparar sus resultados (ISACA, 2013). [22]

Esta metodología ha sido referenciada porque está tomando en cuenta el gobierno de TI de COBIT 5 para dirigir y controlar la empresa hacia el logro de sus objetivos, por medio de agregar valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos.

PMBOK

Es una guía estándar para la dirección de proyectos desarrollada por el Project Management Institute (o PMI), que establece un criterio de buenas prácticas relacionadas con la gestión, la administración y la dirección de proyectos mediante la implementación de técnicas y herramientas que permiten identificar un conjunto de 47 procesos, distribuidos en 5 macroprocesos generales de inicio, planificación, ejecución, control y monitorización, cierre. En cada uno de estos macroprocesos intervienen 10 aspectos clave o áreas de conocimiento, [23]

Esta guía ha sido referenciada porque se toma en cuenta lo descrito en el área de conocimiento de Gestión de las Comunicaciones donde detalla que la gestión de las comunicaciones consta de procesos y actividades organizadas para garantizar la

recopilación, creación, distribución, almacenamiento, recuperación, gestión, control, monitoreo de la información de manera oportuna y eficaz para las partes interesadas. Esta área de conocimiento se utiliza para establecer el proceso de comunicación y consulta del riesgo para el modelo propuesto.

GESTIÓN DE ACTIVOS DE TI: ITAM

La gestión de activos (ITAM, por sus siglas en inglés) es: "Un conjunto de prácticas empresariales que unen funciones financieras, contractuales y de inventario para apoyar la gestión del ciclo de vida y la toma de decisiones estratégicas para el entorno de TI. Los activos incluyen todos los elementos de software y hardware que se encuentran en el entorno empresarial."[24]

Este concepto ITAM ha sido referenciado debido a que no es sólo una herramienta ni un conjunto de procesos, sino que es una disciplina empresarial práctica para la gestión de activos de TI con el fin de que pueden ayudar tanto a líderes como empleados a identificar los eventos que impactan al negocio y a tomar decisiones aún más informadas para restaurar los servicios a los usuarios. Es decir, implementar su gestión manera efectiva le brindará a la compañía los siguientes beneficios:

- Ahorro en costos.
- Reducción de riesgos.
- Incremento en la eficiencia y efectividad de los niveles de servicio.
- Aumento en la satisfación del cliente.

De las metodologías para gestión del riesgo de activos de TI citadas como marco teórico, se concluye que para su contexto de las organizaciones en el sector la metodología Margerit sirve como base para la identificación de activos de la presente investigación por su ventaja principal que existe mayor información pública sobre su aplicabilidad y despliega un orden que determina primero "qué" se quiere proteger, luego establece el "de qué" se quiere proteger, para finalmente decidir el "cómo" se debe proteger los activos de TI, además incorpora como esquema para su metodología fases coincidentes de la ISO 31000 que determina su compatibilidad con la misma.

CAPÍTULO II. MATERIALES Y MÉTODOS

2.1. Tipo y nivel de investigación

La presente investigación es cuantitativa, del tipo descriptiva debido a que se trabajó sobre realidades de hecho y su característica fundamental es la de presentar la una interpretación correcta de las evaluaciones de los procesos relacionados con la investigación su diseño y aplicabilidad del modelo propuesto. Los datos de la prueba para el modelo en mayor porcentaje son retrospectivos (datos históricos) y para las mediciones en el tiempo son prospectivos (obtenidos a partir de los incidentes de seguridad y las evaluaciones posteriores a la construcción del modelo).

2.2. Diseño de investigación

Para la contrastación de la hipótesis se utilizó el método correlacional, este tipo de estudio tiene como objetivo medir el grado de relación que exista entre 2 o más variables (en un contexto particular), este método tiene como valor el observar la reacción de una variable frente al estímulo de la otra y de esa manera comparar el antes y el después.

Este método consiste en: Este método consiste en:

- Una medición de la variable dependiente previa a la aplicación de la variable independiente (Pre – Test)
- La aplicación de la variable independiente.
- Una nueva medición de la variable dependiente, después de la aplicación de la variable independiente (Post – Test)

Como podemos observar:

M1 --------> X --------> M2

Dónde:

M1 = Protección del activo de TI en el sector de distribuidoras de la región Lambayeque antes de la aplicación parcial del modelo.

X = Modelo de gestión de riesgos de tecnologías de información enfocado en estándares adaptados.

M2 = Protección del activo de TI en el sector de distribuidoras de la región Lambayeque después de la aplicación parcial del modelo.

2.3. Población, muestra y muestreo

Se ha considerado una población de cuatro empresas distribuidoras de la región Lambayeque, y como muestra se tomó una empresa en la que se implementó el Modelo de gestión de riesgos.

Se tomaron como elementos de la población a los directores a cargo de las tecnologías de información y personal que da soporte a los servicios de TI; asimismo, documentos claves de área TI como plan estratégico, catálogo de servicios, catálogo de activos, reporte de desempeños de TI.

Cada una de las personas a cargo de los procesos administrativos, se apoyan en las tecnologías de información instaladas.

2.4. Criterios de selección

Se tomaron como criterio de selección el tipo de muestreo por conveniencia, ya que hubo una mayor accesibilidad y proximidad a la muestra, la misma que está conformada por el personal que da soporte a los servicios de TI y administrativos a cargo de los procesos críticos para la organización que son soportados por las tecnologías de información.

2.5. Operacionalización de variables

MODELO DE GESTIÓN DE RIESGOS DE TI ENFOCADO EN ESTÁDARES ADAPTADOS PARA CONTRIBUIR EN LA PROTECCIÓN DEL ACTIVO DE TI EN EL SECTOR DE DISTRIBUIDORAS DE LA REGIÓN LAMBAYEQUE.

Variables	Definición Conceptual	Objetivos Específicos	Dimensiones	Indicadores	Técnica / Instrumento
Variable Independiente: Modelo de Gestión de Riesgos de TI	Esquema adaptado del análisis de diferentes marcos de referencia y metodologías para la gestión de riesgos de TI.	Armonizar estándares, metodologías y herramientas para el análisis y gestión de riesgos de TI, con la finalidad de determinar el modelo.	Metodologías de gestión de riesgos de TI.	Listado de Marcos de Referencia para gestionar los riesgos de TI.	Análisis Documental
		Proponer el modelo de gestión de riesgos adaptado para identificar y abordar los factores de riesgos que afectan el activo de TI en el contexto del sector de distribuidoras.	Gestión de Riesgos de TI.	Listado de los riesgos que pueden afectar a los activos de TI de la organización y el nivel de impacto que pueden tener.	Entrevista, Cuestionarios
		Validar el modelo de gestión de riesgos mediante Juicio de expertos, para valorar el modelo adaptado.	Validaciones.	Propuesta con porcentaje de validez suficiente.	Modelado
Variable Dependiente: Protección del activo de TI	Capacidad de los activos de TI para abordar los factores de riesgos.	Implementar el modelo de gestión de riesgos de TI para contribuir en la protección del activo de TI aplicado en un caso de estudio.	Validaciones.	Propuesta con porcentaje de validez suficiente.	Modelado

Tabla 1: Indicadores y operacionalización de variables

2.6. Técnicas e instrumentos de recolección de datos

En la investigación se empleó múltiples técnicas e instrumentos de recolección de información.

Variable	Técnicas	Instrumentos
Contribuir en la protección del activo de TI en el sector de distribuidoras de materiales de construcción.	Encuesta	Cuestionario Entrevistas
	Observación	Documentos Estratégicos

Tabla 2: Métodos, técnicas e instrumentos

2.7. Procedimientos

Se elaboró un cuestionario o test de preguntas para medir qué prácticas de gestión de riesgos en el sector de distribuidoras de materiales de construcción de la región Lambayeque. Para su elaboración se ha considerado como criterio gestión de riesgos de TI en su APO: 12 de COBIT 5. Así mismo se tomaron en cuenta las diversas metodologías con respecto al tema.

Cuestionarios. - Se elaboró cuestionarios para el personal de TI, gerentes de áreas y usuarios claves de la empresa, esto nos ayudó a obtener información de cómo se vino ejecutando la gestión de riesgos de TI en la organización de estudio.

Observación. - Se elaboró fichas de revisión de datos de cada documento. Los documentos revisados fueron:

De la Empresa caso de estudio:

a. Plan Estratégico empresarial

De la Jefatura de Tecnologías de la Información.

a. Plan estratégico de TI.

b. Plan anual de TI.

c. Sistema de Gestión de Seguridad de la Información.

d. Manual de gestión de riesgos operativos de TI.

2.8. Plan de procesamiento y análisis de datos

Los datos fueron recogidos en forma manual, para luego, procesar la información utilizando el software Microsoft Excel 2016, con el cual obtuvimos cuadros y gráficos estadísticos que sirvieron para el análisis y son presentados en el presente documento.

2.9. Consideraciones éticas

- Informados a los participantes sobre el propósito de la investigación.
- Guardar la confidencialidad y anonimato de los participantes cuando se solicite.
- Respeto al lugar donde se efectúa la investigación.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Diagnóstico del sector

En el desarrollo del producto acreditable de la presente investigación, se hizo un análisis a las empresas del sector con el fin de obtener información de las prácticas de gestión de riesgo en las distribuidoras de artículos de ferretería, acabados y materiales de construcción de la región Lambayeque se desarrolló un cuestionario de 16 preguntas basado en el marco de COBIT 5 en su proceso habilitador APO: 12 para la gestión de riesgos TI y consideraciones de otras metodologías para gestión del riesgo en activos de TI como Margerit y Octave (Ver Anexo 1: Cuestionario). El cuestionario referenciado fue aplicado al personal del área de TI en 4 empresas del sector (Ver Anexo 4) las mismas que a solicitud de los encuestados por consentimiento informado y criterios de ética para la publicación de la presente investigación se cuidará la denominación de cada organización las cuales en adelante para la descripción e interpretación de los resultados obtenidos denominaremos Distribuidora A, Distribuidora B, Distribuidora C, Distribuidora D.

De la información recopilada en las encuestas se pudo observar que el 50% de las empresas conformada por la distribuidora A y distribuidora D consideran la gestión de riesgo en su planificación empresarial en términos muy generales, no desarrollan de manera práctica la gestión de riesgos en todas las áreas de su organización, el otro 50% de los encuestados afirman que la gestión del riesgo aplica únicamente en áreas específicas. El 75% de las áreas de TI dependen de su gerencia general y el 25% depende de un área de finanzas, el 100% cuentan con un plan estratégico de TI, pero solo la distribuidora B y distribuidora C que representan el 50% ha realizado inventario de los activos de TI, incluyendo el personal de soporte, infraestructura, servicios, etc. El otro 50% implementa un inventario limitados a equipos informáticos.

Las funciones del área de TI de las empresas en estudio se alinearon a las metas del proceso de gestión del riesgo que indica COBIT con el fin de determinar su práctica actual, el cual permite identificar que: Si bien el 100% del personal de TI posee las competencias y habilidades adecuadas para cumplir con su función, solo el 50% conformado por la distribuidora B y C analiza, gestionan y reportan los riesgos de TI, además la información obtenida evidencia que nada más la distribuidora B que

representa el 25% ha estimado efectivamente la pérdida económica que traen consigo eventos de riesgo de TI, el 50% validan los resultados de análisis de riesgos antes de usarlos como solución (Distribuidora B y C), las mismas que conforma el 50% de las distribuidoras que reporta y coordina los riesgos con la alta dirección.

Con respecto al nivel de riesgo de TI que se asume para cumplir con los objetivos del negocio el 50% la distribuidora B y C afirma que ha definido estos parámetros.

El 100% de los encuestados, indica que no emplea estándares y metodologías nacionales e internacionales que apoye a una efectiva gestión de riesgos; por lo tanto, se visualiza una incertidumbre de confiabilidad en las prácticas de gestión de riesgo que se implementa.

El 50% conformado por la distribuidora B y C promueve una cultura consciente de los riesgos TI e impulsa a la empresa a una identificación proactiva e impactos potenciales en el negocio.

El 50% ha identificado que servicios de TI son esenciales para sostener la operación de los procesos de negocio, analiza sus dependencias y eslabones débiles.

El 25% indica que el ambiente de su centro de datos es el adecuado para proteger sus activos de TI y el otro 75% aún no implementa un ambiente adecuado.

El 75% evalúa y actualiza los factores de riesgos de TI con una frecuencia semestral y el otro 25% con frecuencia trimestral.

El 50% de organizaciones evidencia que no destina dentro de su plan de inversiones presupuesto para una permanente gestión de riesgos se indica que implementa inversión cuando ya se presentaron eventos de riesgos conocidos, el otro 50% de inversiones se destinan a riesgos generales del negocio con seguros para cubrir escenarios en infraestructura de locales e inventario de mercadería.

Para ver los resultados de las encuestas (Ver Anexo 5)

3.2 Análisis de estándares, marcos de trabajo, metodologías relacionados con el tema

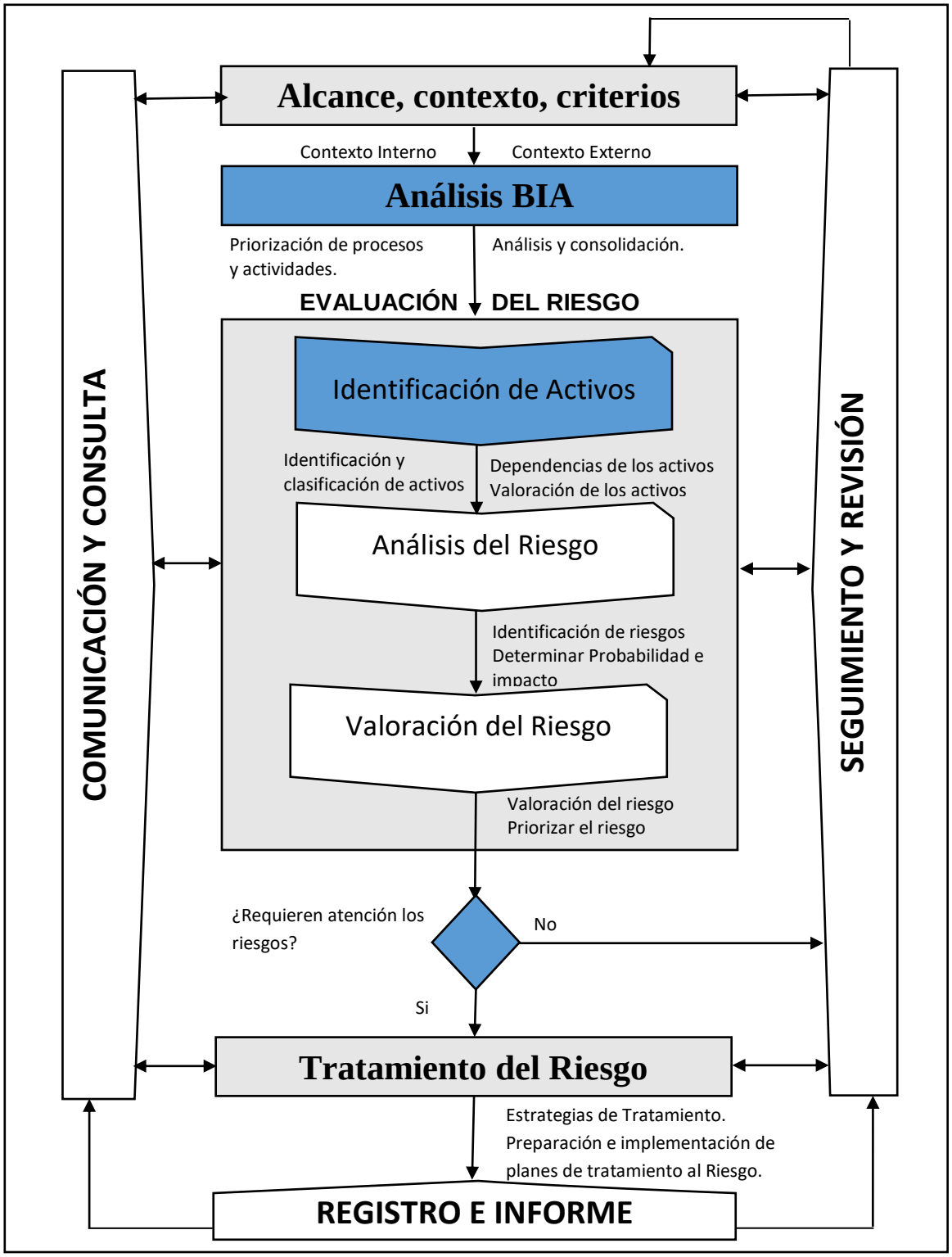
En este capítulo se analizó los estándares y metodologías referentes a la gestión de riesgos en tecnologías de información. El capítulo incluye un análisis conceptual y un cuadro comparativo armonizado de los estándares básicos para gestión de riesgos en

organizaciones así como metodologías que implementan un enfoque integral en activos de TI, cuadros que sirvieron para identificar fases coincidentes y aportaciones en gestión de riesgos y confieran en la realización de la propuesta del modelo según las necesidades y realidad del sector de distribuidoras de artículos de ferretería, acabados y materiales para la construcción (Ver anexo 7 y 8).

En la figura Nª 9, se establece el modelo propuesto de gestión de riesgo de la investigación que incluye como base fases y directrices de la norma ISO 31000:2018 y adaptada un Análisis BIA por la particularidad en un entorno comercial Retail que es de vital importancia la continuidad de sus operaciones. El Análisis BIA apoyará a identificar procesos y actividades críticas del negocio que requieran priorización en la organización, fase que no se incluye los estándares referidos originalmente en ISO 31000:2018 y Margerit. El análisis BIA cederá priorizar los riesgos que enfrentan los activos de TI y así mismo permitirá cumplir con los objetivos de la organización y una efectiva inversión para la implementación de gestión de riesgos.

También, en el modelo propuesto se adapta la fase de evaluación de riesgo para la identificación de activos de TI que implementa la metodología Margerit con el fin de realizar las estrategias de tratamientos de riesgos que protejan los activos TI y contribuyan con mantener los servicios que soportan los procesos y actividades del negocio. Por último se añade antes de la etapa de tratamiento un punto decisorio que permitirá a la organización tomar la decisión si el riesgo identificado debe pasar a fase de tratamiento.

Figura 9: Modelo de Gestión de Riesgo propuesto tomando como referencia ISO 31000: 2018 y Margerit para protección de activos de TI



Fuente: Elaboración propia.

3.3 Desarrollo de las fases del modelo propuesto

Fase I: Alcance, Contexto y criterio

Esta fase es el pilar de la norma ISO 31000:2018 y su propósito es definir el alcance de la gestión de riesgo comprendiendo el contexto en que opera la organización en su entorno interno y externo, además de definir los criterios y parámetros para el proceso de la gestión del riesgo. Un elemento a destacar es el alcance del análisis, incluyendo obligaciones propias y obligaciones externas.

1. **Alcance:**

   En este punto la organización deberá definir el alcance de sus actividades de gestión del riesgo. Si el proceso de la gestión del riesgo se aplica a niveles distintos (por ejemplo: estratégico, operacional, financiero, de programa, de proyecto u otras actividades), además se debe determinar el objetivo del alcance y el equipo de trabajo para la evaluación de riesgos describiendo sus roles y responsabilidades; todo ello alineado con los objetivos de la organización.

2. **Establecimiento del contexto:**

   El contexto en un proceso de gestión del riesgo se deberá establecer a partir de la comprensión de los entornos interno y externo en los cuales opera las distribuidoras de artículos de ferretería, acabados y materiales de construcción.

2.1. Contextos Internos

a) Cultural: Se define como el conjunto de conocimientos que permite identificar las características de las empresas distribuidoras de la región Lambayeque, para definir los escenarios de comportamiento conformado por actitudes, experiencia, creencias y valores propios de la organización y las partes interesadas internas (personal de operaciones, administrativos, gerentes, etc.).

Fuentes de información: Plan estratégico, visión, misión, objetivos estratégicos, cultura organizacional, políticas corporativas, organigrama de institución, modelo operativo empresarial, etc.

b) Estructura Organizacional: Se define como el conjunto de componentes organizacionales que agrupan para formar áreas, departamentos de acuerdo a su función que permite gestionar su actividad y recursos, que para el caso de empresas distribuidoras son de tipo vertical con estructuración colaborativa entre los empleados y directivos.

   Fuentes de Información: Organigrama corporativo.

c) Recursos: Se define como el conjunto de activos tecnológicos que dan soporte a los procesos de las organizaciones comerciales como software, servidores, equipos de cómputo, equipos de red, sistema de protección eléctrica, etc.

   Fuentes de Información: Inventario de infraestructura tecnológica.

d) Metas y objetivos: Se define como el conjunto de ideas empresariales que apuntan al crecimiento, servicio al cliente, retención, rentabilidad y eficiencia operativa en empresas comerciales.

   Fuentes de Información: Plan Estratégico.

2.2. Contextos Externos

a) Ámbito de negocio: es un conjunto de elementos que tienen el potencial de afectar su economía y desempeño de las distribuidoras comerciales en la región Lambayeque, como los proveedores de productos y servicios, competencia directa.
   Fuente de información: Análisis FODA de la organización, lista de proveedores de productos y servicio de transporte, convenios establecidos con empresas externas.

b) Ámbito Sociocultural: es un conjunto de elementos referentes al estilo de vida, el contexto geográfico, demográfico, etc. relacionado a los grupos de interés como clientes con obras de construcción, constructoras, distribuidores ferreteros, gobiernos locales y otros organismos de la región.
Fuente de información: Datos de licencias de construcción municipal, Organismo supervisor de las contrataciones del estado (OSCE), gobiernos locales.

c) Ámbito legal: son las exigencias legales y reglamentarias, donde los riesgos de incumplimiento pueden poner en juego a la organización, como normas tributarias, laborales.
Fuente de información: SUNAT, INDECI, SUNARP, INDECOPI, MTPE, etc.

d) Ámbito económico: es un conjunto de elementos y entidades relacionados con la economía, la situación fiscal, las variaciones en los precios, evolución de tasas de interés, tasa de cambio, las distintas políticas fiscales y monetarias a nivel nacional e internacional.
Fuentes de Información: SBS, BANCA, BCRP.

e) Ámbito tecnológico: Este ámbito está compuesto generalmente por factores que tienen que ver la rapidez de las innovaciones, el grado de desarrollo de tecnologías de información en organizaciones de distribuidoras.
Fuentes de Información: Revistas, evolución tecnológica, casos de éxitos en Retail, etc.

3. **Criterio:**

La organización deberá precisar la cantidad y el tipo de riesgo que puede o no puede tomar con relación a los objetivos estratégicos, valorando la importancia del riesgo a los niveles operacional, legal, financiero, económico, reputacional, ambientales, políticos, etc., como soporte para priorizar las decisiones.

Riesgos Operacionales:

Es aquél que puede provocar pérdidas como resultado de errores humanos, procesos internos inadecuados o defectuosos, fallos en los sistemas como consecuencia de acontecimientos externos.

Riesgos legales:

Se refiere a los obstáculos legales o normativos que pueden obstaculizar el rol de una empresa en un sitio determinado.

Riesgos financieros:

Son todos aquellos relacionados con la gestión financiera de las empresas. Es decir, aquellos movimientos, transacciones y demás elementos que tienen influencia en las finanzas empresariales: inversión, diversificación, expansión, financiación, entre otros. En esta categoría es posible distinguir algunos tipos:

- Riesgo de crédito.
- Riesgo de tasas de interés.
- Riesgo de mercado.
- Riesgo gestión.
- Riesgo de liquidez.
- Riesgo de cambio.

Riesgos económicos:

En este caso, se refiere a los riesgos asociados a la actividad económica, ya sean de tipo interno o externo. En el primer caso, hablamos de las pérdidas que puede sufrir una organización debido a decisiones tomadas en su interior. En el segundo, son eventos cuyo origen es externo. Para diferenciarlo del ítem anterior, es preciso señalar que el riesgo económico afecta básicamente a los beneficios monetarios de las empresas, mientras que los financieros tienen que ver con todos los bienes que tengan las organizaciones a su disposición.

Riesgo reputacional:
Es toda acción, evento o situación que podría impactar negativa o positivamente en la reputación de una organización.

Riesgos ambientales:
Son aquellos a los que están expuestas las empresas cuando el entorno en el que operan es especialmente hostil o puede llegar a serlo. Tienen dos causas básicas: naturales o sociales.

Riesgos políticos:
Este riesgo puede derivarse de cualquier circunstancia política del entorno en el que operen las empresas. Los hay de dos tipos: gubernamentales, legales y extralegales.

Fase II: Análisis BIA

En esta fase se realizará el análisis de impacto al negocio – BIA, que dará como resultado consideraciones importantes para la gestión del riesgo en las distribuidoras de la región Lambayeque. El análisis BIA permitirá clasificar los procesos del negocio de acuerdo a su criticidad, estableciendo un orden o escala de prioridad para la ejecución de actividades que se requieran en la recuperación o restablecimiento del proceso, además permitirá definir la estimación del tiempo que la organización puede tolerar, en caso de un incidente o desastre que le impida operar normalmente.

Para elaborar el análisis BIA se toma como referencia la norma ISO 22317-2015 de la cual se tiene en cuenta las siguientes etapas:

a. Priorización de procesos y actividades: En esta etapa debemos incluir a los dueños del proceso y alta gerencia de la organización para acordar la prioridad de los procesos y actividades críticas e importantes que permitan la continuidad y estabilidad de la organización en el momento de una interrupción. La priorización ayudará a la organización a identificar los procesos o actividad de mayor y menor

impacto además de un calendario por franjas horarias definidas teniendo en cuenta la ausencia del mismo con el objetivo de destinar el esfuerzo y recursos para la recuperación después del incidente.

b. Análisis y consolidación: En esta etapa la organización debe realizar un análisis final o consolidación de análisis del proceso BIA. Esto implica: revisar los resultados de las actividades de priorización y sacar conclusiones que conduzcan a los requisitos de continuidad del negocio.

Las siguientes tablas permiten realizar el impacto de análisis sobre el negocio (BIA) de las empresas distribuidoras de la región Lambayeque.

Tabla de definición de los parámetros de evaluación.

Identificación de Impactos			
1.1. Impactos Económicos			
	Peso->	**25%**	
	Descripción	**Magnitud del Impacto Económico Operativo (Miles S/)**	**Magnitud del Impacto Económico Operativo (Miles S/)**
		Límite Inferior (Mayor o igual que)	**Límite Superior (Menor o igual que)**
1	Insignificante	S/ 0	S/30,000
2	Menor	S/ 30,001	S/ 50,000
3	Moderado	S/ 50,001	S/200,000
4	Mayor	S/200,001	S/ 1,000,000
5	Catastrófico	S/ 1,000,001	
1.2. Impactos Operacional			
	Peso->	**30%**	
	Descripción	**Impacto operacional a nivel de proceso**	
1	Insignificante	Afecta menos del 10% de las actividades normales del proceso	
2	Menor	Afecta entre el 10% y el 30% de las actividades normales del proceso	
3	Moderado	Afecta entre el 30% y el 50% de las actividades normales del proceso	
4	Mayor	Afecta entre el 50% y el 80% de las actividades normales del proceso	
5	Catastrófico	Afecta más del 80% de las actividades normales del proceso	
1.3. Impactos Legal			
	Peso->	**25%**	
	Descripción	**Impacto legal a nivel de proceso**	
1	Insignificante	Si el proceso no está disponible no se produce incumplimiento de normas, regulaciones o procesos contractuales	
2	Menor	Si el proceso no está disponible podría existir una probabilidad de que se generen incumplimientos de normas, regulaciones, multas y reclamos pero no tiene un impacto importante en el negocio.	
3	Moderado	Si el proceso no está disponible genera incumplimiento con regulaciones o contratos importantes, pero se puede dar el escenario de no recibir multas o sanciones significativas.	
4	Mayor	Si el proceso no está disponible genera sanciones y multas importantes por incumplimiento de la normatividad aplicable.	
5	Catastrófico	Si el proceso no está disponible genera sanciones y multas que pueden generar pérdidas financieras o el cierre temporal de la organización.	
1.4. Impactos Reputacional			
	Peso->	**20%**	
	Descripción	**Impacto reputacional a nivel de proceso**	
1	Insignificante	Si el proceso no se encuentra disponible no afecta la imagen de la empresa.	
2	Menor	Si el proceso no se encuentra disponible podría afectar la imagen de la empresa.	
3	Moderado	Si el proceso no se encuentra disponible afecta la imagen que se tiene de la empresa	
4	Mayor	Si el proceso no se encuentra disponible afecta la imagen de la empresa y pone en ventaja competitiva la competencia	
5	Catastrófico	Si el proceso no se encuentra disponible afecta totalmente la imagen de la empresa, se pierde posicionamiento e imagen.	

Tabla 3: Definición de los parámetros de evaluación soporte para el Análisis BIA
Fuente: Elaboración Propia.

Definición del RTO: El tiempo de recuperación objetivo (RTO), define el tiempo máximo de recuperación de una aplicación de tal forma que el impacto no afecte a la organización. Encontrar el RTO es definir el punto de equilibrio entre el costo de la estrategia de recuperación y las perdidas por el impacto de la no disponibilidad, si el RTO es muy pequeño entonces las perdidas por el impacto también son pequeñas sin embargo el costo de la estrategia de recuperación es alto, por el contrario, si el RTO es muy grande, el costo de la estrategia de recuperación es pequeño, pero las pérdidas por el impacto de la no disponibilidad son altas.

Rango de Tiempo de Interrupción Tolerable
Entre 0 y 1 Horas
Entre 1 y 4 Horas
Entre 4 y 8 Horas
Entre 8 y 24 Horas
Superior a 24 Horas

Tabla 4: Rango de RTO propuesto
Fuente: Elaboración Propia.

Es el punto en el tiempo en el cual los datos deben ser recuperados después de una interrupción de los sistemas. Este parámetro permite establecer estrategias efectivas de respaldo y alta disponibilidad de las plataformas tecnológicas y sistemas críticos.

Definición del RPO: Punto de recuperación Objetivo (RPO) de los sistemas fueron definidos bajo la siguiente clasificación:

- Punto de Fallo: Al recuperarse los sistemas después de una interrupción, los datos deben ser recuperados exactamente en el punto en que se encontraban al momento del fallo o interrupción.
- Cierre de Día: Después de una interrupción los sistemas deben ser recuperados con los datos del cierre del día anterior.

- Cierre de Semana: Después de una interrupción los sistemas deben ser recuperados con los datos del cierre semanal.

Para cada uno de los procesos, se define el RPO de los sistemas críticos que lo soportan. Cuando varios procesos tienen RPO diferentes para el mismo sistema, se escoge el RPO más bajo.

Punto en el cual deben ser recuperados los datos
Entre 0 y 1 Horas
Entre 1 y 4 Horas
Entre 4 y 8 Horas
Entre 8 y 24 Horas
Superior a 24 Horas

Tabla 5: Rango de RPO propuesto
Fuente: Elaboración Propia.

Los valores definidos para los parámetros de evaluación de tiempos y punto de recuperación se obtuvieron a partir del análisis de 3 empresas distribuidoras de la región Lambayeque referido por los antecedentes, las características y a la exigencia de la operación considerando los efectos para cada espacio de tiempo que estuviera detenido el proceso.

CUADRO DE IDENTIFICACIÓN DE PROCESOS				
Num. Proceso	**CODIGO PROCESO**	**PROCESO**	**ÁREA O DEPARTAMENTO**	**DEPENDENCIA SERVICIOS DE TI**
1	[P_Compras]	Proceso de Compras	Logística	Módulo de gestión de compras.
2	[P_Importación]	Proceso de Importación	Logística	Módulo de Importaciones.
3	[P_Inventario]	Proceso de Inventario	Inventarios	Módulo de gestión de inventarios.
4	[P_Tesorería]	Proceso de Gestión de Tesorería	Tesorería	Módulo de caja y bancos.
5	[P_Contabilidad]	Proceso de Contable	Contabilidad	Módulo de contabilidad
6	[P_Ventas]	Proceso de Ventas	Ventas	Módulo de gestión de ventas.
7	[P_Distribución]	Proceso de Distribución y Despacho.	Ventas	Módulo de distribución y despacho de mercadería.
8	[P_Créditos]	Proceso de Créditos	Créditos y Cobranzas	Módulo de gestión de créditos.
9	[P_Cobranza]	Proceso de Cobranza	Créditos y Cobranzas	Módulo de gestión de cobranzas.
10	[P_Planillas]	Proceso de Planillas	RRHH	Módulo de RRHH.
11	[P_ServCliente]	Gestión del Cliente	Ventas	Módulo de CRM.
Fecha:		**Realizado Por:**		**Aprobado Por:**

Tabla 6: Plantilla de identificación de procesos
Fuente: Elaboración Propia.

La Tabla Nª:6, permitirá desarrollar la identificación de los procesos de negocio para el análisis BIA y el cual cederá en la siguiente tabla a identificar por cada proceso las actividades críticas e importantes que desea priorizar de acuerdo a su misión y objetivos de las organizaciones, además asistirá a encontrar la relación de cada proceso y actividad con los servicios de TI, definir los requisitos de RTO y RPO tolerables para el proceso frente a su inactividad y su calificación de impacto para el negocio.

CUADRO DE ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)													
CODIGO PROCESO	**ACTIVIDAD**	**IMPACTOS ACUMULATIVOS POR HORAS**										**CATEGORIA**	**CLASIFICACIÓN**
		RTO (Horas)					**RPO (Horas)**						
		0-1	**1-4**	**4-8**	**8-24**	**>24**	**0-1**	**1-4**	**4-8**	**8-24**	**>24**		
[P_Compras]	Solicitud o Requerimiento de Compra	1	1	2	3	4	1	1	3	4	5	OPERACIONAL	MENOR
	Evaluación y Selección de Proveedores											OPERACIONAL	MENOR
	Carga y actualización de precios											OPERACIONAL	MENOR
[P_Importación]	Solicitud o Requerimiento de Compra internacional											OPERACIONAL	MENOR
	Distribución de productos importados.											OPERACIONAL	MENOR
[P_Inventario]	Recepción de compra de mercadería											OPERACIONAL	MENOR
	Toma Inventario											OPERACIONAL	MENOR
[P_Tesorería]	Liquidación de cobranza diaria											ECONÓMICO	MODERADO
	Pagos a Proveedores											ECONÓMICO	MODERADO
	Generar Pago de Planillas											REPUTACIONAL	MODERADO
[P_Contabilidad]	Registro de facturas de compras											OPERACIONAL	MENOR
	Declaración de rentas e impuestos											LEGAL	CATASTRÓFICO
[P_Ventas]	Búsqueda de Clientes y Toma de Pedidos											OPERACIONAL	MENOR
	Gestión de Ventas											ECONÓMICO	CATASTRÓFICO
[P_ Distribución]	Despacho de Productos											OPERACIONAL	MODERADO
[P_Cobranzas]	Gestión de Créditos											OPERACIONAL	MODERADO
	Gestión de Cobranzas											ECONÓMICO	MODERADO
[P_Planillas]	Procesamiento de Planillas											REPUTACIONAL	MODERADO
Fecha:		**Realizado Por:**							**Aprobado Por:**				

Tabla 7: Plantilla de priorización de procesos y actividades
Fuente: Elaboración Propia.

La Tabla Nª:7, permitirá desarrollar y clasificar las actividades críticas e importantes para el objetivo del proceso con el fin de destinar esfuerzo y recursos más específicos en el mismo. La valoración del impacto se definió teniendo en cuenta la ausencia de la actividad por franjas de horas definidas en RTO y RPO (ver los rangos propuestos de RTO y RPO para el sector de distribuidoras tabla N° 4 y 5), la valoración del impacto se establece en la escala del 1 a 5, siendo 1 el de menor y 5 el de mayor impacto que cede visualizar un mapa de colores sobre su afectación del proceso o actividad al transcurrir el tiempo (ver calificación tabla Nª 3: Definición de parámetros de evaluación).

Listado de procesos críticos identificados

Número proceso	Proceso	Actividades por proceso	Actividades Priorizadas
1	Proceso de ventas.	**3**	**2**
2	Proceso de Almacén.	**3**	**1**
3	Proceso de reparto	**2**	**1**
4	Proceso de cierre de caja	**4**	**2**
5	Proceso de compra nacionales	**3**	**1**

Tabla 8: Plantilla de análisis y consolidación
Fuente: Elaboración Propia.

En la tabla N° 8, asistirá a consolidar los procesos y actividades críticas para la organización que permitirá su enfoque a orientar el análisis de riesgo.

Fase III: Evaluación del Riesgo

En esta fase se analiza los riesgos que afrontan los activos de TI y que podrían impedir que las organizaciones de distribuidoras de la región Lambayeque no logren sus objetivos. El objetivo del proceso es valorar los riesgos para establecer medidas o controles de salvaguardas.

Esta fase contempla las siguientes actividades:

3.1 Identificación de activos:

Esta actividad tiene como objetivo identificar y clasificar los activos de TI, que dan soporte a la operatividad de distribuidoras de la región Lambayeque, así mismo permite establecer las dependencias entre activos con el objetivo de identificar como un activo superior depende de otro activo inferior. Finalmente se valoran los activos por criticidad que dan soporte al core del negocio de estas organizaciones.

Los activos de TI, en una organización de distribuidoras, hacen referencia a cualquier elemento que contenga información y permita prestar un servicio. Se plantea los siguientes tipos de activos tomando en cuenta las recomendaciones de la Metodología Margerit:

Tipos de Activos de TI

Etiqueta	Tipo de Activo	Función
[ED]	Edificación e instalaciones físicas	Soporte
[HW]	Hardware (Equipamiento informático)	Soporte
[AP]	Aplicaciones (Software)	Aplicación
[COM]	Redes de comunicaciones	Soporte
[MEDIA]	Medios de almacenamiento extraíble	Soporte
[IE]	Información electrónica	Datos
[IP]	Información en papel	Datos
[RH]	Recursos Humanos	Soporte
[S]	Servicios prestados	Servicio
[P]	Procesos de negocio	Proceso

Tabla 9: Tipos de activos de TI
Fuente: Basado en recomendaciones de Margerit v3 libro I.p.22-24

a) Clasificación de los activos

La siguiente tabla se estructura para iniciar con la identificación de los activos de información, revise primeramente la tabla de clasificación para cada uno de las categorías indicadas anteriormente.

Ítem	Tipo de Activo	Activo de TI	Código Activo	Función
1	[ED]	Centro de datos principal	[ED_CDatos]	Soporte
2	[HW]	Servidor de aplicaciones	[HW_SrvApli]	Soporte
3	[HW]	Servidor de base de datos	[HW_SrvBD]	Soporte
4	[HW]	Servidor de correo electrónico	[HW_SrvMail]	Soporte
5	[HW]	Servidores de seguridad	[HW_SrvSeg]	Soporte
6	[HW]	Servidor de terminales remotas	[HW_SerTerm]	Soporte
7	[AP]	Sistema de base de datos	[AP_BD]	Aplicación
8	[AP]	Sistema de gestión Comercial	[AP_SCom]	Aplicación
9	[AP]	Sistema de gestión de RRHH	[AP_SRRHH]	Aplicación
10	[HW]	Dispositivos de comunicación	[COM_DisCom]	Soporte
11	[MEDIA]	Discos de almacenamiento externo	[MED_DExt]	Soporte
12	[IE]	Archivos electrónicos	[IE_File]	Datos
13	[IE]	Códigos fuente	[IE_CodFuente]	Aplicación
14	[IE]	Códigos Ejecutable	[IE_CodEjec]	Aplicación
15	[IP]	Documentos	[IP_Doc]	Datos
16	[RH]	Personal de TI	[RH_PTI]	Soporte
17	[S]	Servicio de Gestión Comercial	[S_GesCom]	Servicio
18	[S]	Servicio Web	[S_PWeb]	Servicio
19	[S]	Servicio de Intranet	[S_Intranet]	Servicio
20	[S]	Servicio de Wifi	[S_Wifi]	Servicio
21	[S]	Servicio de Acceso a Internet	[S_Internet]	Servicio
22	[S]	Servicio de Correo Electrónico	[S_EMail]	Servicio
23	[S]	Servicio de Telefonía	[S_Tele]	Servicio

Tabla 10: Plantilla de registro de los activos de TI por tipo de activo
Fuente: Elaboración Propia

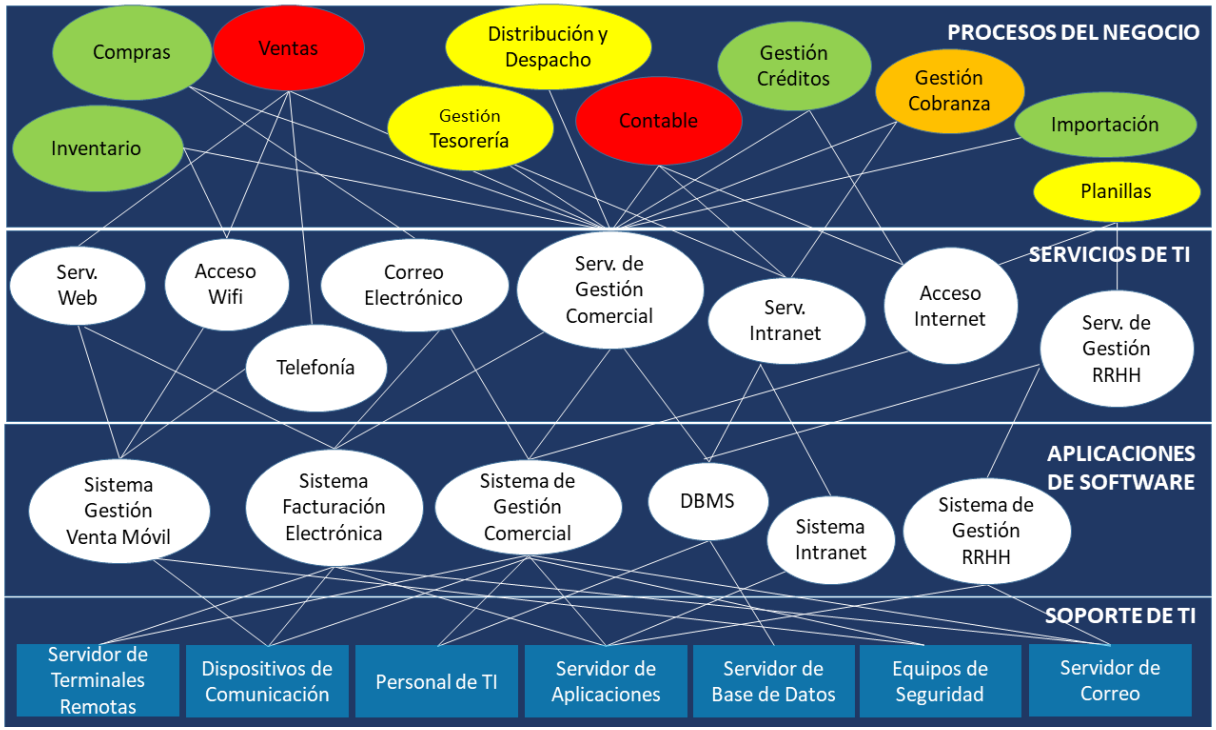
b) Dependencias de los activos

En esta actividad, se estable una relación de dependencia entre los activos TI. Para establecer la relación de dependencia de activos se debe tener en cuenta los procesos identificados en la fase del análisis BIA (Ver tabla Nª 7) y su clasificación de activos por su función (Ver tabla Nª 09,10) con el fin de evaluar que activos son esenciales para la sostenibilidad de los procesos de negocio.

Para descubrir y modelar su dependencia se recomienda empezar poniendo en lo más alto la información representada por los procesos de negocio y los

servicios de TI que dan sostenibilidad a estos procesos. Para su ilustración se toma en cuenta Margerit en su caso práctico para modelar las dependencias entre activos para la prestación de servicios (Ilustración 21), así también se considera para el diseño de la figura Nª 10 las recomendaciones descritas en la publicación de investigación de M. Arangurí, en su fig.3: Dependencia de activos [20].

Figura 10: Dependencia de activos



Fuente: Basado en recomendaciones de Margerit v3 libro I. p.91

En la figura Nª 10 se adicionan los procesos de negocio identificados en análisis BIA con un color establecido que representa visualmente la priorización que se debe tener con el proceso según el tipo de impacto que genera para la organización en sus operaciones de negocio además de su dependencia con los activos de TI desde un enfoque a nivel de servicios, aplicaciones de software y soporte.

c) Valoración de los activos

Una vez inventariado los activos de TI en esta etapa es necesario designar un valor que la organización tiene para el activo de TI desde la perspectiva de la necesidad de proteger si estos llegaran a dañarse, perderse o difundirse, es decir, pues más valioso será un activo por las pérdidas ocasionadas para la organización y por el cual se debe tener mayor nivel de protección de las dimensiones de seguridad. Para la asignación en términos de protección que requieren las empresas distribuidoras de la región Lambayeque se propone definir 3 dimensiones.

Para la valoración, se recomienda usar la Escala de valoración de Likert, que permite a través de rangos del 1 al 5 establecer nivel de conformidad con respecto a los criterios que se esperan, para la disponibilidad, integridad y confidencialidad.

Confidencialidad (C): propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos.
Integridad (I): propiedad de salvaguardar la precisión y totalidad de los activos.
Disponibilidad (D): propiedad de estar disponible y utilizable por solicitud de una entidad cuando lo necesite.

	Valor	Criterio
Confidencialidad (C)	5	Los daños serían catastróficos, la reputación y la imagen de la institución se verían comprometidas.
	4	Los daños serían relevantes, el incidente implica a otros procesos
	3	Daños bajos, el incidente no trasciende del proceso afectado.
	2	Daños muy bajos, el incidente no trasciende del proceso afectado.
	1	No aplica / No es relevante

Tabla 11: Valores de criterios de Confidencialidad

	Valor	Criterio
Integridad (I)	5	Tiene que estar correcto y completo al menos en un 95.5%
	4	Tiene que estar correcto y completo al menos en un 75%
	3	Tiene que estar correcto y completo al menos en un 50%
	2	No es relevante los errores que tenga o la información que falte
	1	No aplica / No es relevante

Tabla 12: Valores de criterios de Integridad

	Valor	Criterio
Disponibilidad (D)	5	Debe estar disponible al menos el 95.5% del tiempo
	4	Debe estar disponible al menos el 75% del tiempo
	3	Debe estar disponible al menos el 50% del tiempo
	2	Debe estar disponible al menos el 10% del tiempo
	1	No aplica / No es relevante

Tabla 13: Valores de criterios de Disponibilidad

Los niveles de criticidad de los activos de TI se obtendrán del producto de la sumatoria de las calificaciones realizadas para cada criterio de seguridad (Ver tablas 11, 12, 13) y se clasificarán de la siguiente manera:

Rango	Nivel de criticidad	Descripción		Criterio
1-3	1	Muy Bajo	MB	Irrelevante para la operación de los proceso comerciales.
4-6	2	Bajo	B	Afecta la operación de los procesos comerciales en 10%, no implica pérdida de información.
7-9	3	Medio	M	Afecta la operación de los procesos comerciales en 50%, no implica pérdida de información.
10-12	4	Alto	A	Afecta la operación de los procesos comerciales en 75%, puede implicar pérdida de información.
13-15	5	Muy Alto	MA	Paraliza la operación de los procesos comerciales en 95% e implica perdida de información.

Tabla 14: Niveles de criticidad de los activos de TI

Como podemos observar en la Tabla N° 14 los valores de rango fueron definidos de 1 al 15 donde 15 es el valor máximo obtenido de las sumatoria de las calificaciones realizadas en los criterios de seguridad.

Nivel de Criticidad = Confidencialidad + Integridad + Disponibilidad

Para el registro y la valoración de la criticidad de los activos de TI se utilizará la siguiente plantilla:

Etiqueta Categoría	Código Activo	N° Activo	Descripción	Criterios de Seguridad			Total	Nivel de Criticidad
				C	I	D		
[ED]		1		5	2	3	10	Alto [A]
[HW]		2		4	4	5	13	Muy Alto [MA]
[AP]		3		3	1	5	9	Medio [M]

Tabla 15: Plantilla de criterios de criticidad de activos
Fuente: Elaboración Propia

3.2 Análisis del riesgo:

En esta etapa, el propósito principal del análisis de riesgos es poder identificar las deficiencias, debilidades y carencias que tiene la organización en los diferentes procesos de TI relacionados a la protección de los activos que han sido identificados. El resultado de esta actividad permitirá determinar cuáles son las debilidades internas más relevante y menos relevante que pueden ser aprovechadas por las amenazas que al materializarse generan resultados impactantes sobre los activos de TI y afectan los procesos de negocio para la empresa (Ver Mapa de dependencias figura 10).

a) Identificar el riesgo

Para realizar esta actividad se recomienda realizar el análisis de riesgos inicialmente por medio de técnicas como entrevistas, cuestionarios, lluvia de ideas, juicios de experiencia y los registros, cuestionarios y grupos de trabajo que

permitan organizar las posibles condiciones o situaciones que se pueden presentar y poner en peligro los activos de TI.

Dado que el modelo propuesto se caracteriza por presentar a los activos de TI y su impacto a los procesos de negocio, se propone una forma que permitan identificar el riesgo de cada uno del activo su amenaza y vulnerabilidad.

IDENTIFICACIÓN DEL RIESGO						
N° Activo	Categoría	Activo	Amenaza	Vulnerabilidad	Riesgo	
					Código	Evento /consecuencias
1	Etiqueta de la categoría del activo	Nombre del Activo	Descripción de las amenazas	Descripción de Vulnerabilidades encontradas	Código del riesgo (R1, R..)	Descripción del evento o consecuencias de riesgo que genera de las vulnerabilidades identificadas

Tabla 16: Plantilla para identificar riesgos
Fuente: Elaboración Propia

b) Determinar probabilidad e impacto

Esta actividad permitirá valorizar la materialización de cada una de las amenazas identificadas para cada activo de TI, tomando como referencia las vulnerabilidades encontradas para cada una de ellas. La valorización de las amenazas se realizará en base a la calificación de sus dos componentes principales, como son: la probabilidad de su ocurrencia y el impacto que pueden ocasionar.

Para la realización de dicha valorización, el estándar ISO 27005 propone métodos con los cuales se puede llevar a cabo la valorización de riesgos de manera adecuada. Dado que el modelo propuesto se caracteriza por presentar a riesgos en los activos de TI y su impacto a los procesos de negocio.

Tablas de nivel de valorización

Para la estimación de la probabilidad de ocurrencia de cada una de las amenazas consideradas se utilizará la siguiente tabla que define los niveles de probabilidad de ocurrencia o frecuencia de las amenazas.

Nivel	Probabilidad	Descripción
1	Raro	No se presenta en varios años.
2	Improbable	Se podría presentar una vez al año.
3	Posible	Se podría presentar hasta tres veces al año.
4	Probable	Se podría presentar mensualmente.
5	Casi Seguro	Se podría presentar a diario.

Tabla 17: Valoración de los niveles de Probabilidad
Fuente: Basado en recomendaciones de Margerit v3 libro I.p.28

Para la estimación del impacto de cada una de las amenazas identificadas se utilizará la siguiente tabla que define los niveles de impacto de las amenazas:

Nivel	Impacto	Descripción
1	Muy Bajo	Tiene un efecto adverso insignificante en las operaciones o activos de la organización.
2	Bajo	Tiene un efecto adverso limitado en las operaciones o activos, de la organización.
3	Medio	Tiene un efecto adverso considerable que ralentiza operaciones o activos de la organización.
4	Alto	Tiene un efecto adverso grave o catastrófico que paraliza algunas operaciones o activos críticos de la organización.
5	Muy alto	Tiene un efecto adverso grave o catastrófico que paraliza todas las operaciones o activos críticos de la organización.

Tabla 18: Valoración de los niveles de impactos
Fuente: Basado en recomendaciones de Margerit v3 libro I.p.28

3.3 Valoración del riesgo.

El propósito de la fase de valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios de riesgo establecidos en el ámbito de las distribuidoras de la región Lambayeque para determinar cuándo se requiere una acción adicional porque provocan incertidumbres al logro de los objetivos.

a) Valorar el Riesgo

Para esta actividad, se propone una estructura de semaforización con el fin que permita resaltar mediante colores la clasificación de los riesgos identificados por su relevancia, de manera rápida y amigable.

En la tabla 19, para determinar el riesgo potencial de una amenaza se optó por realizar una matriz de calor tomando como referencia la valorización en función de los criterios de probabilidad e impacto. Si podemos observar, el riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta para el tratamiento.

Riesgo= Probabilidad x Impacto

PROBABILIDAD	VALOR	1	2	3	4	5
CASI SEGURO	5	5	10	15	20	25
PROBABLE	4	4	8	12	16	20
POSIBLE	3	3	6	9	12	15
IMPROBABLE	2	2	4	6	8	10
RARO	1	1	2	3	4	5
	IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO

Tabla 19: Matriz de la valorización de probabilidad por impacto de las amenazas
Fuente: Propia

NIVEL DE RIESGO	CALIFICACIÓN
MUY ALTO	15 A 25
ALTO	9 A 14
MEDIO	4 A 8
BAJO	1 A 3

Tabla 20: Tabla de Categoría del Riesgo
Fuente: Propia

En la siguiente tabla 21, permitirá realizar la valorización de los riesgos que se detectaron de la etapa anterior de análisis de riesgos (tabla 16) vinculado con la categoría del riesgo definida (tabla 20), la misma que fue resultado de los criterios de probabilidad e impacto de las amenazas.

VALORIZACIÓN DEL RIESGO						
Código	PROBABILIDAD		IMPACTO		Evaluación Del Riesgo	CATEGORÍA
	Nivel	Descripción	Nivel	Descripción		
R1	3	Posible	5	Muy Alto	**15**	**Muy Alto**
R2	2	Improbable	4	Alto	**8**	**Medio**
R3	4	Probable	3	Medio	**12**	**Alto**
R4	4	Probable	3	Medio	**12**	**Alto**
R5	1	Raro	3	Medio	**3**	**Bajo**

Tabla 21: Plantilla de Valoración del Riesgo
Fuente: Propia

Los resultados de la valoración del riesgo se deberían registrar, comunicar y luego validar a los niveles apropiados de la organización.

b) Priorizar el riesgo

Para esta actividad, primero se ubican los riesgos identificados en la etapa anterior (Tabla N° 16) y su valorización del riesgo (Tabla N° 22), para elaborar un mapa de calor donde los riesgos son ubicados en las zonas de prioridades (Tabla N° 22) con el objetivo de visualmente apoyar a facilitar la toma de decisiones para el tratamiento de los riesgos que se desarrollará en la siguiente fase de tratamiento.

Tabla 22: Matriz de priorización de riesgos

PROBABILIDAD						
	5: Casi Seguro					
	4:Probable			R3/R4		
	3: Posible					R1
	2: Improbable				R2	
	1: Raro			R5		
		1. Muy Bajo	2.Bajo	3.Medio	4.Alto	5.Muy Alto
		IMPACTO				

Entorno de control del riesgo

Para llevar a cabo un entorno de control de los riesgos la alta dirección de la organización deberá determinar tres elementos principales que integre a un posterior tratamiento basado en sus límites de tolerancia, apetito y capacidad.

Elementos que permitirá contrastar la adecuación de los riesgos que se afronta tomado como referencia su declaración de misión, visión y valores; su estrategia corporativa, el activo y su relación con el proceso para declarar si puede ser tolerable o debe ser tratado.

Según la ISO (Guide 73:2009, 2009) define los siguientes conceptos:

- Apetito: Cantidad y tipo de riesgo que una organización está dispuesta a buscar o asumir.
- Tolerancia: Cantidad de riesgo que podría llegar a asumir la organización.
- Capacidad: Es el riesgo máximo asumible sin comprometer los objetivos.

La siguiente tabla recoge los riesgos identificados por la empresa en orden de prioridad y permitirá establecer la declaración de los elementos descritos.

RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R1	Muy Alto	[ED_CDatos]	Centro de datos.	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico)	20	10	15	Debe ser tratado
R5	Bajo	[AP_SBDErp]	Centro de datos.	Abuso de privilegios de acceso.	Falta de procedimientos de validación de consultas.	12	6	12	Aceptable

Tabla 23: Plantilla matriz de priorización y control de riesgos
Fuente: Propia

Fase IV: Tratamiento del Riesgo

En esta etapa se determinan e implementan las estrategias de protección (mitigar, evitar, trasferir, aceptar) para gestionar los riesgos anteriormente analizados. Estas acciones se realizan junto con un plan de acción en donde se definen recursos, responsabilidades para finalmente definir las políticas a seguir.

4.1. Estrategias de Tratamiento

Para determinar las estrategias se toma como referencia la información de la priorización y control requerido para gestión de riesgos (Tabla N° 23), para determinar la estrategia del tratamiento.

"La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra costos, esfuerzo o desventajas de la implementación ", ISO (31000, 2018).

Las opciones de tratamiento como posibles estrategias fueron definidas según la ISO 31000: 2018 y consideraciones de la 27005: 2018.

- Modificar-Mitigar: Ejecutar acciones para prevenir y controlar la probabilidad o frecuencia e impacto de los riesgos. Implementar procesos de gestión de riesgos para introducir, eliminar, modificar controles que permitan que el riesgo residual puede ser reevaluado como aceptable.
- Evitar: cuando se decide no emprender o dejar de realizar actividades que da lugar a una acción riesgosa, pero puede ser una elección sumamente costosa para la organización.
- Transferir-Compartir: se refiere a asegurar y equilibrar los riesgos, compartiéndolos con terceros que pueda manejar el riesgo en particular de manera más efectiva. Por ejemplo, se puede realizar mediante un seguro que cubra las consecuencias, o mediante la subcontratación de un socio cuyo rol es monitorear y tomar acciones inmediatas para detener un ataque antes de que ocurra.

- Retención-Aceptar: aceptar el cierto riesgo de un modo costo efectivo, es decir se conoce el riesgo y se establece la decisión de conservar el riesgo sin tomar medidas adicionales. Está estrategia será viable si la organización controla el riesgo y vigile que este no aumente.

4.2. Preparación e implementación de los planes de tratamiento del riesgo

En esta actividad, el propósito de los planes de tratamiento del riesgo es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera tal que los involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planificado. El plan de tratamiento debería identificar claramente el orden en el cual el tratamiento del riesgo se debería implementar.

La información proporcionada en el plan del tratamiento debería incluir:

- Las acciones propuestas de tratamiento.
- El fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados.
- Las personas que rinden cuentas y aquellas responsables de la aprobación e implementación del plan.
- Los recursos necesarios, incluyendo las contingencias.
- Los plazos previstos para la realización y la finalización de las acciones.
- Presupuesto para implementar los controles de salvaguardas.

Para realizar el tratamiento de riesgos, se debe revisar cada uno de los activos y sus amenazas identificadas en las fases anteriores, además se debe proponer acciones que permitan implementar una estrategia de respuesta al riesgo cuyo objetivo es reducir la probabilidad de ocurrencia o el impacto sobre los procesos de negocio.

Cada una de las acciones para el tratamiento de riesgos debe trabajarse como proyectos o acciones individuales, es importante considerar la inversión necesaria

para cada proyecto, el cual debe estar sustentado en función al impacto sobre los procesos de negocio y actividades identificados en BIA como críticos para sostener las operaciones del negocio y su recuperación del servicio en empresas distribuidoras comerciales.

PLANES DE TRATAMIENTO DEL RIESGO											
Código: **Nombre del Proyecto:** _____			**Fecha de elaboración:** _____ **Elaborado Por:** _____					**Revisado Por:** _____ **Fecha:** _____			
RIESGO			**PLAN DE TRATAMIENTO**								
Código	**Cód. Activo**	**Nivel**	**Tratamiento**	**Acciones**	**Puntaje Aceptable**	**Objetivo**	**Responsable**	**Recursos**	**Proceso Afectado**	**Tiempo de ejecución**	**Presupuesto**
Riesgo en orden de prioridad	Código del activo a tratar	Nivel del riesgo que está expuesto el activo.	Estrategia de tratamiento	Acciones a realizar para operativizar el proyecto	Puntaje esperado del Riesgo luego del tratamiento (Apetito)	Objetivo / Resultado costo-beneficio del proyecto	Persona (s) responsable por implementación de la opción de tratamiento	Recursos requeridos / Contingencias	Identificador o descripción del Proceso Afectado.	Tiempo de ejecución de implementación	Presupuesto requerido para implementar proyecto.
R1											
R3											
R4											
R2											
R5											

Tabla 24: Plantilla para definir planes de tratamiento del riesgo
Fuente: Propia

Tabla Nª 24 permitirá realizar un registro de los planes de tratamiento para cada riesgo identificado, así mismo se establecerá el presupuesto requerido para la implementación de controles según el tipo de tratamiento seleccionado.

Fase V: Comunicación y consulta

En esta fase, el propósito de la comunicación y consulta es asistir a las partes interesadas a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo en un lenguaje común de negocio, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones. Una coordinación cercana entre ambas debería facilitar un intercambio de información basado en hechos, oportuno, pertinente, exacto y comprensible, teniendo en cuenta la disponibilidad, confidencialidad e integridad de la información.

La comunicación y consulta pretende:

- Reunir diferentes áreas de experiencia para cada etapa del proceso de la gestión del Riesgo.
- Asegurar que se consideren de manera apropiada los diferentes puntos de vista cuando se definen los criterios del riesgo y cuando se valoran los riesgos.
- Proporcionar suficiente información para facilitar la supervisión del riesgo y la toma de Decisiones.
- Construir un sentido de inclusión y propiedad entre las personas afectadas por el riesgo.

Para esta fase de comunicación y consulta se implementa la siguiente plantilla (ver tabla Nª 25), la cual toma en consideración elementos del área de conocimiento de gestión de las comunicaciones de la guía del PMBOK 6ta edición.

PLAN DE GESTIÓN DE COMUNICACIÓN Y CONSULTA							
Proceso de comunicación	**Descripción de Actividad**	**Emisor**	**Receptor(es)**	**Resultado de la comunicación (Información)**	**Aprobado por**	**Periodo de vigencia**	**Canal de comunicación**
Describe el flujo de información. **Entradas:** son documentos o información para el proyecto. **Proceso:** consiste en obtener la retroalimentación de información entre el director del proyecto y los interesados. En esta etapa se utilizan herramientas y técnicas para la presentación formal de información y documentación del análisis. **Salidas:** incluye informes de resultados de información requerida por los interesados.	Descripción de la actividad a realizar en el proceso de comunicación y consulta (parte o contenido de agenda).	El emisor es aquella fuente que genera mensajes de interés. Responsable de comunicar.	Es el agente (persona o grupo) que recibe el mensaje.	Documento de Informe y/o correo electrónico. Documento: Acta de reunión, etc.	Persona responsable de la aprobación de los resultados de la comunicación	Periodo o frecuencia de tiempo que se estable la comunicación.	Medio o canal de transmisión de la comunicación.

Tabla 25: Plantilla para el plan de gestión de comunicación y consulta
Fuente: Propia

Fase VI: Seguimiento y Revisión

En esta fase, el propósito es asegurar y mejorar la calidad e la eficacia de la implementación de gestión del riesgo además de evaluar periódicamente los cambios que puedan modificar o invalidar la evaluación del riesgo. Esto incluye recopilar, analizar información, registrar resultados y proporcionar retroalimentación.

En este proceso se recomienda revisar los cambios en los contextos internos, externos, modificaciones en los catálogos de procesos, servicios, aplicaciones de software, soporte de TI y mapa de dependencias de activos que durante su frecuencia de seguimiento y revisión de resultados con el tiempo puedan variar en aspectos de cambio de probabilidad e impacto.

SEGUIMIENTO Y REVISIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS		
RIESGO	**Código:**	
	Nombre del Proyecto:	
	Riesgo que se trata:	
	Nivel máximo de criticidad de los activos que se trata:	
PLAN DE TRATAMIENTO	**Estrategía de riesgo:**	
	Acciones a realizar:	
	Puntaje acceptable:	
	Objetivo:	
	Responsable:	
	Recursos:	
	Proceso Afectado (Identificador/Nombre)	
	Tiempo de ejecución	
	Presupuesto	
SEGUIMIENTO Y REVISIÓN	**Verificación de Resultados:**	**Indicadores**
	Acciones a ejecutar para la revisión de la eficacia del proyecto o proceso.	Determinar el indicador de medición.
	Análisis de Resultados	
	Acciones para mejorar el proyecto (Retroalimentación)	

Tabla 26: Plantilla de seguimiento y revisión del plan de tratamiento de riesgos
Fuente: Adaptado de la publicación de M. Arangurí "Modelo de Gestión de Riesgos de TI..," [pág.64-65]

En la tabla Nª 26 pretende facilitar al gestor de riesgos el proceso de seguimiento y revisión de los riesgos, el cual toma la ficha de identificación de los resultados de auditoria de proyectos para verificar y actuar en un ciclo Deming (PDCA) de mejora continua para afrontar nuevos eventos de riesgos variantes por variación en probabilidad e impacto.

Fase VII: Registro e informe

El propósito de esta fase, es documentar e informar el proceso de la gestión del riesgo, los resultados y lecciones aprendidas, así también la decisión de tratamiento del riesgo que se emprende.

Con el registro e informe se pretende:

- Comunicar las actividades de la gestión del riesgo y sus resultados a la organización.
- Proporcionar información para la toma de decisiones.
- Mejorar las actividades de la gestión del riesgo.
- Asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

El informe es una parte integral de la gobernanza de la organización y debería mejorar la calidad del diálogo con las partes interesadas, y apoyar a la alta dirección y a los órganos de supervisión a cumplir sus responsabilidades.

REGISTRO E INFORME											
Código:											
Nombre del Proyecto:											
Preparado por:											
Fecha:											
Lección Aprendida Nro.: *numero correlativo*											
Lección Aprendida: *nombre que sugiera e identifique la decisión de tratamiento del riesgo o lección aprendida.*											
Rol en el Equipo del Proyecto: *nombre y rol de la persona que toma la decisión de tratamiento o informa la lección aprendida.*											
Fase del Proceso: *		Identificación de Procesos		Evaluación del Riesgo		Valoración del Riesgo		Tratamiento		Seguimiento y Revisión	
Proceso o actividad de Negocio Afectado**:**											
¿Resultados de actividades ejecutadas de la gestión del riesgo?											
¿Cuál es la lección específica aprendida? *Enunciar la lección aprendida solo si se ejecutó acciones de tratamiento al riesgo mitigar, evitar, transferir.*											
¿Qué acción se tomó y por qué? *Enunciar solo si la opción de tratamiento seleccionada es Aceptar el riesgo.*											
¿Qué comportamiento se recomienda para el futuro?											
¿Quién debe ser informado sobre esta lección aprendida?: (marcar una)											
		Sponsor		Gerente(s) Proyecto		Equipo del		Todo el Personal			
		Otros:									
¿Cómo debe ser distribuida esta lección aprendida? (marcar todas las que apliquen)											
		e-mail		Intranet/pagina Web		Preguntas Frecuentes		Biblioteca			
		Otros:									
¿Ha anexado referencia(s), ejemplo(s) y/o material(es) adicional(es)?		si		no							
Nombre(s) de anexo(s): 1. 2.											

Tabla 27: Plantilla de registro e informe de tratamiento del riesgo y lecciones aprendidas
Fuente: Propia

En la tabla Nª 27 pretende apoyar al gestor de riesgos para llevar un registro de las decisiones de tratamiento para la gestión de riesgo que se implementa y los resultados obtenidos como lecciones aprendidas de los controles implementados.

DISCUSIÓN

De acuerdo al objetivo general planteado, en la presente tesis para contribuir en la protección del activo de TI en sector de distribuidoras de la región Lambayeque, se desarrolló el modelo de gestión de riesgos de TI basado en estándares adaptados.

Para la validación del modelo se diseñó dos instrumentos: Por juicio de expertos, el cual fue aplicado a cuatro profesionales expertos en el tema que validaron la estructura y contenido del modelo propuesto en la presente tesis obteniendo la aceptación del mismo (ver Anexo N° 10).

Para medir el nivel de confiabilidad del instrumento aplicado para la obtención de los resultados, se procesó el Método de Alfa de Cronbach y para evaluar el nivel de concordancia de los jueces en la validez del contenido se realizó la prueba de Kendall como se muestran en las siguientes tablas.

Standardized coefficients (Y):						
Source	**Value**	**Standard error**	**t**	**Pr > |t|**	**Lower bound (95%)**	**Upper bound (95%)**
ToothPaste-T1	0.010	0.000				
ToothPaste-T2	0.132	0.153	0.820	0.416	-0.219	0.322
ToothPaste-T3	0.824	0.183	4.268	0.202	0.413	1.215
ToothPaste-T4	0.510	0.193	2.721	0.166	0.219	1.451
			Kendall	**0.784**	**A.C.**	**0.762399**
Standardized coefficients (Whiteness):						
Source	**Value**	**Standard error**	**t**	**Pr > |t|**	**Lower bound (95%)**	**Upper bound (95%)**
Toothpaste-T1	0.000	0.000				
Toothpaste-T2	0.132	0.193	1.830	0.516	-0.229	0.132
Toothpaste-T3	0.834	0.183	4.568	0.200	0.443	0.335
Toothpaste-T4	0.510	0.183	2.741	0.213	0.129	0.311
			Kendall	**0.929**	**A.C.**	**0.778**

Tabla 28: Estadística de confiabilidad y concordancia con ANOVA

ANÁLISIS DE VARIANZA						
Origen de variación	**S.C**	**G.L**	**P.C**	**F**	**Proba.**	**Criterios**
Filas	0.849	0.123	0.464	9.595	0.330	6.944
Columnas	0.036	0.434	0.148	2.184	0.219	6.944
Error	0.098	0.420	0.049			
Total	**0.982**	**0.977**				
	Kendall	**A.C.**				

Tabla 29: Estadística de confiabilidad y concordancia con Minitab

Leyenda de datos:

S.C: Grado de confiabilidad

G. L: Grado de libertad

P.C: Fuente confiable

F: Factor de confiabilidad

Proba: Probabilidad

Criterios: Criterios de rango

Para la estadística resultante del coeficiente de Cronbach se tiene como criterio general, George y Mallery (2003, p. 231) los cuales sugieren las recomendaciones siguientes para evaluar los coeficientes:

- Coeficiente alfa Cronbach mayor a 0.9 es excelente
- Coeficiente alfa Cronbach mayor a 0.8 y menor a 0.9 es bueno
- Coeficiente alfa Cronbach mayor a 0.7 y menor a 0.8 es aceptable
- Coeficiente alfa Cronbach mayor a 0.6 y menor a 0.7 es cuestionable
- Coeficiente alfa Cronbach mayor a 0.5 y menor a 0.6 es pobre
- Coeficiente alfa Cronbach menor a 0.5 es inaceptable

La medida obtenida del coeficiente de confiabilidad de Cronbach es de 0.977 con un nivel de confiabilidad excelente.

Para la estadística el coeficiente de concordancia de Kendall, el valor oscila entre 0 y 1. Donde el valor de 1 significa una concordancia de acuerdos total y el valor de 0 un desacuerdo total. La tendencia a 1 es lo deseado pudiéndose realizar nuevas rondas si en la primera no alcanza significación en la concordancia. Tomando en consideración lo mencionado, el modelo propuesto alcanza un valor de concordancia de 0.982 lo que significa que existe un alto nivel de concordancia entre jueces.

Finalmente, de la combinación de los resultados de los dos métodos aplicados para la evaluación, se puede demostrar que existe un alto nivel de concordancia entre los cuatro evaluadores y por el valor obtenido con la aplicación del método de Alfa de Cronbach, el modelo alcanza un nivel de excelente.

Luego de la validación del modelo se procede a contrastar la hipótesis analizando los siguientes indicadores:

Indicador 1: Número de activos críticos de TI identificados que pueden afectar la operación de la organización.

En la evaluación de la situación problemática que motivó el desarrollo de la presente investigación, se encontró que las empresas distribuidoras de la región Lambayeque carecían de un modelo práctico organizado soportado en estándares relevantes que les permita realizar un inventario de activos críticos de TI y su relación de dependencia con los procesos de operación comercial, a fin de que se pueda determinar que tiene la organización y que podría pasar si este activo se ve afectado.

En la ejecución del modelo propuesto aplicado al caso de estudio de la empresa distribuidora SAC de Lambayeque, bajo un enfoque de simplicidad y flexibilidad, se mostró como resultado (Tabla Nº 16: Criticidad de activos) la identificación de 26 activos críticos que de acuerdo a su clasificación se agruparon en los siguientes activos 01 de edificación, 07 de hardware, 08 de software, 01 de información electrónica, 01 de

almacenamiento externo, 01 documentos físicos, 01 de recursos humanos, 06 de servicios, lográndose identificar la dependencia que existe entre ellos así como los requerimientos de confidencialidad, disponibilidad e integridad.

Indicador 2: Número de riesgos detectados en los activos de TI que soportan los procesos de negocio.

Como resultado de la evaluación de la situación actual de gestión de riesgos en las empresas del sector de distribuidoras de la región Lambayeque los miembros de los grupos de interés involucrados, manifiestan tener información de la existencia de estándares y metodologías de gestión de riesgos de TI, sin embargo resultan alta complejidad y requieren asignar personal exclusivo para su aplicación y monitoreo.

Para medir el indicador de número de riesgos detectados por activo crítico, se implementó para el caso de estudio el modelo propuesto debidamente validado por juicio de expertos (ver Anexo N° 10) lográndose la identificación de 85 riesgos de los cuales, a través de la aplicación de 05 plantillas de trabajo, se logró determinar que 7 eran de tratamiento prioritario por ser calificados como de riesgo muy alto y 16 riesgos de alta a media prioridad, los cuales afectan a la operación de los procesos de gestión comercial soportados por TI.

Indicador 3: Cantidad de proyectos propuestos para el tratamiento de los riesgos.

En la evaluación de la situación problemática del contexto actual de gestión de riesgos en la empresas del sector de distribuidoras de la región Lambayeque los miembros de los grupos de interés involucrados, revelaron que para enfrentar alguna amenaza, se adoptaban respuestas de carácter reactivo después de concretarse el hecho que generaban altos costos de corrección y no se contaban con proyectos justificables y organizados que permitan ser presupuestados con anticipación para presentación los responsables de las tomas de decisiones de la empresa.

La ejecución del modelo propuesto en la presente tesis, aplicado al caso de estudio, mostró como resultado (Tabla N° 21) la identificación de 85 riesgos, de los cuales 7 fueron considerados de muy alta prioridad y 16 riesgos de alta a media prioridad, por exceder los límites de tolerancia planteados por la empresa, que serían mitigados a través de la ejecución de 5 proyectos en el proceso de tratamiento de los mismos.

CONCLUSIONES

- Se valoró la implementación del modelo de gestión de riesgos en los activos de TI, aplicándolo en un caso de estudio en la Empresa Distribuidora A. S.A.C de la región Lambayeque, verificando contribuir en la protección de sus activos que soportan los procesos de gestión comercial, como resultado se logró identificar 85 riesgos y apoyar a una efectiva toma de decisiones para minimizar los impactos de operación, económicos y legales.

- Así también, con la aplicación del modelo de gestión de riesgos de TI desarrollado en la presente tesis, en el caso de estudio, se logró formular 5 proyectos que permiten dar tratamiento a 23 riesgos que fueron considerados 7 de muy alta prioridad y 16 riesgos de alta a media prioridad, por exceder los límites de tolerancia planteados por la empresa, promoviendo de esta manera una toma de decisiones de carácter proactivo y evitando el comportamiento reactivo que encamina consigo costos de corregir los efectos de un riesgo de TI materializado.

- La gestión de los riesgos en las organizaciones del sector de distribuidoras debería considerarse un proceso intrínseco, ya que si la empresa no conoce sobre el riesgo que corren sus activos de TI difícilmente llegará a estar preparada para evitar una posible ocurrencia, de allí la importancia de conocerlo y crear controles para disminuir o eliminar la ocurrencia.

- Como consecuencia del análisis realizado, se entiende lo vital que es contar con una infraestructura tecnológica que permita ir incorporando mejoras en los servicios de TI. Concluyendo que la mejor forma de potenciar su rendimiento y disponibilidad es contar con soluciones capaz de mantener una alta disponibilidad del core del negocio.

REFERENCIAS BIBLIOGRÁFICAS

- [1] ISO, ISO 31000:2018(es) "Risk management— Guidelines," U.S. Patente ISO, 2018 Disponible en: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en. [Accedido: 20-agosto-2018].
- [2] L.M. Romeral y A. TORRES., "Gestión de los Riesgos Tecnológicos", *Revista de procesos y métricas de las tecnologías de la información*, vol.5, no.1, pp.1-9, enero de 2008.
- [3] Foro Económico Mundial, "Informe de Riesgo Mundial 2018, 13ª Edición", Foro Económico Mundial, Ginebra, Suiza, 2018.
  Disponible en: https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/the-global-risks-report-2018-es.pdf. [Accedido: 20-agosto-2018]
- [4] Deloitte, "Cyber Risk: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?", Deloitte, S.L, Madrid, junio 2017.
  Disponible en: http://perspectivas.deloitte.com/hubfs/Campanas/WannaCry/Deloitte-ES-informe-WannaCry.pdf [Accedido: 20-agosto-2018],
- [5] A. Casas, "La gestión del riesgo se especializa en el año 2018", Revista ComputerWorld, suplemento nro. 1353, pp. 94-100. ISSN: 0212-2456, España, marzo 2018.
- [6] Deloitte, "La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información", Encuesta 2016 sobre Tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica, julio, 2016.
  Disponible en: https://www2.deloitte.com/pe/es/pages/risk/articles/la-evolucion-de-la-gestion-de-ciber-riesgos-y-seguridad.html. [Accedido: 20-agosto-2018],
- [7] E. Chong, "18va Encuesta Global de CEOs Pwc Perú", Revista PricewaterhouseCoopers, primera edición, pp. 12-16, Perú, 2015.
- [8] Numa Arellano, "La gestión de riesgos como pilar del Gobierno Corporativo", Artículo resultados de la encuesta "Gobierno, riesgo y cumplimiento 2015", de EY. Perú, 2016.
  Disponible en: https://www.ey.com/pe/es/newsroom/newsroom-am-gestion-riesgos-gobierno-corporativo. [Accedido: 20-agosto-2018],

- [9] C. Y. Romero, "Modelo integrado de gestión de riesgos de seguridad en los departamentos de TIC", tesis de master, Univ. De Especialidades Espíritu Santo UEES, Samborondón, Ecuador, 2017.
- [10] M. Arangurí, R. Imán y G. León, "Modelo de Gestión de Riesgos de TI basados en estándares adaptados a las TI que soportan los procesos para contribuir a la generación de valor en las Universidades Privadas de la Región Lambayeque", tesis de master, Univ. Católica Santo Toribio de Mogrovejo, Chiclayo, Perú, 2016.
- [11] E.Chillogallo y V. Zambrano, "Elaboración de un Modelo de Gestión de Riesgos de Tecnologías de Información para la Fiscalía General del Estado de Quito", tesis de master, Univ. Politécnica Nacional, Quito, Ecuador, 2016.
- [12] M. Fernanda, "Propuesta de un Plan de Gestión de Riesgos de Tecnología aplicado en la Escuela Superior Politécnica del Litoral", tesis de master, Univ. Politécnica de Madrid, Madrid, España, 2015.
- [13] G. Vanegas y C. Pardo, "Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT Towards a IT risks management model for MSME", Revista S&T de Univ. EAFIT, Vol. 12(30), pp. 35-48, 2014.
- [14] D. Moncayo, "Modelo de evaluación de riesgos en activos de TIC's, para pequeñas y medianas empresas del sector automotriz", tesis de master, Escuela Politécnica Nacional, Quito, Ecuador, 2014.
- [15] ISACA. "COBIT® 5: Un Marco de Negocio para el Gobierno y la Gestión de la Empresa," U.S. Patente IL 60008 ISBN 978-1-60420-282-3, abril, 2012.
- [16] ISO, ISO/IEC 27005:2011. Information technology -- Security techniques -- Information security risk management. U.S; Patente ISO, 2011.
- [17] British Standard, "Risk management – Code of practice and guidance for the implementation of BS ISO 31000," London, Reino Unido, Patente BSI, junio 2011. Disponible en: https://shop.bsigroup.com/ProductDetail?pid=000000000030228064. [Accedido: 19-enero-2019],
- [18] COSO, "Enterprise Risk Management Integrating with Strategy and Performance," U.S. Patente P254469-01 0516, Junio 2017.

- [19] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I - Método", Ministerio de Hacienda y Administraciones Públicas, Madrid, octubre 2012.
  Disponible: https://administracionelectronica.gob.es/. [Accedido:19-enero-2019],
- [20] R. A. Caralli, J. F. Stevens, L. R. Young y W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", Carnegie Mellon University, Software Engineering Institute, Rep. Téc. CMU/SEI-2007-TR-012, Mayo 2007.
- [21] CRAMM (CCTA Risk Analysis and Management Method). Disponible en: http://evaluries.blogspot.com/2014/03/herramienta-de-evaluacion-de-riesgo.html. [Accedido:19 -enero -2019].
- [22] ISACA. "COBIT 5 for risk," U.S. Patente IL 60008 ISBN 978-1-60420-458-2, Octubre 4, 2013.
- [23] Proyect Management Institute. "PMBOK GUIDE SIX EDITION" U.S. Patente ISBN 9781628253924, Septiembre 30, 2017.
- [24] InvGate. "Comenzando con la Gestión de Activos de TI", Enero, 2018. Disponible en: https://info.invgate.com/hubfs/White%20Papers/ES/InvGate%20Asset%20Management%20WP%20ES.pdf?hsLang=es. [Accedido: 03-agosto-2019].

ANEXOS

Anexo1: Encuestas de diagnósticos aplicadas

Cuestionario De Gestión De Riesgos De Ti Dirigido A Personal Del Área De Informática

Objetivo de Encuesta: Realizar un análisis de la cultura y prácticas de gestión de riesgos en el sector de distribuidoras dedicadas a venta y distribución de artículos de ferretería, acabados y materiales para la construcción.
Fecha:
Nombre de la empresa:
Giro del Negocio:
Nombre del encuestado:
Cargo/e-mail/teléfono:
CAPACIDAD DE LA EMPRESA EN TECNOLOGIA DE LA INFORMACIÓN Y COMUNICACIONES
Asigne con una "X" la(s) capacidad(es) que su empresa presenta en términos de metodología, normalización y avaluación de conformidades: ( ) Empresa tiene Planeamiento Estratégico a largo Plazo; ( ) Empresa ha definido e implementado el Gobierno Corporativo; ( ) Empresa cuenta con Gobierno de Tecnologías de Información; ( ) Empresa ha implementado la Gestión de Riesgos en los procesos del negocio;
GESTIÓN DE RIESGOS
Asigne con un número su respuesta: 1. ¿En qué medida su organización considera el riesgo como parte del proceso de Planificación empresarial? [ ] 1. Términos muy generales en toda la empresa. 2. Sólo en áreas específicas. 3. Ninguna.
2. ¿En el organigrama de la Institución de quién depende el área de TI?

A. Directorio Ejecutivo ( ) B. Gerencia General ( ) C. Gerencia Financiera ( ) D. Gerencia de Operaciones ( ) E. Otros ( ) Especificar:_____
3. ¿Cuenta con un plan estratégico de TI? Si ( ) No ( )
4. ¿Se ha realizado inventario de los activos de TI, incluyendo el personal de soporte, infraestructura, servicios, planes y registros de manuales críticos? Si ( ) No ( )
5. ¿Los riesgos relacionados con los activos de TI están identificados, analizados, gestionados y reportados? Si ( ) No ( ) Especificar la opción elegida que práctica implementa: _____
6. ¿La empresa ha estimado la pérdida económica asociada con escenarios de riesgo de TI que afectan a la disponibilidad del servicio? Si ( ) No ( )
7. ¿El personal de TI posee las competencias y habilidades adecuadas para cumplir con su función? Si ( ) No ( ) ¿Cuáles son los parámetros de medición que Ud. Aplica con su personal? _____
8. ¿Validan los resultados de análisis de riesgos antes de usarlos para la toma de decisiones de mitigación y respuesta al riesgo? Si ( ) No ( )
9. ¿Los riesgos de TI son informadas y coordinadas con la alta dirección de la empresa? Si ( ) No ( )

10.- ¿La empresa ha determinado el nivel de riesgos relacionados con TI que está dispuesta a asumir para cumplir con sus objetivos? Si ( ) No ( )
11. ¿Se ha determinado si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes? Si ( ) No ( )
12. ¿Se promueve una cultura consciente de los riesgos TI e impulsa a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio? Si ( ) No ( )
13. ¿Se ha identificado qué activos, servicios y recursos de TI son esenciales para sostener la operación de procesos de negocio, analizar dependencias y eslabones débiles? Si ( ) No ( )
14. ¿El centro de datos y cuartos de comunicaciones cuentan con ambientes apropiados para su correcto funcionamiento? (aire acondicionado, área mínima, sistema de protección eléctrico, extintores, piso técnico, falso techo, etc.) Si ( ) No ( )
15. ¿Con que frecuencia se evalúa y actualiza los factores de riesgo de TI? A. Mensual ( ) B. Trimestral ( ) C. Semestral ( ) D. Anual ( )
16. ¿Desde la perspectiva de la planificación de inversiones, hay una partida en el presupuesto para cualquiera de los siguientes? [ ] 1. Administración de riesgos para TI. 2. Administración de riesgos de negocio. 3. Ambos, Administración de riesgos de negocios y TI. 4. No existe partida para administración de Riesgos de Negocios o TI.

Encuesta interna para medir los activos de la información dirigida a personal del área de informática de la empresa distribuidora local

Cargo: ……

Se ha diseñado el presente cuestionario para el personal del área de informática, Con la finalidad de llevar buen proceso de medición sobre las Tecnologías de Información, por lo que necesitamos de su colaboración. Marcar con una (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

Leyenda: 5. Siempre 4. Casi Siempre 3. A veces 2. Casi nunca 1. Nunca

	DIMENSIONES	ESCALA				
		1	2	3	4	5
	Procesos					
1	Se ha establecido políticas para el uso adecuados de los activos de información (Base de Datos, Hardware, software, archivos físicos, etc.)					
2	Se han establecido controles para el uso adecuado de los activos de información (Base de Datos, Hardware, software, archivos físicos, etc.)					
3	Se cumple con las políticas establecidos en el uso adecuado de los activos de información (Base de Datos, Hardware, software, archivos físicos, etc.)					
	¿Se han establecido procedimientos para el resguardo de la información?					
4	¿Se han establecido políticas para el acceso al servicio de internet?					
5	¿Establecen y aplican políticas para el uso adecuado de contraseñas de seguridad?					
6	¿Se tiene un registro codificado de las incidencias que se presentan en el manejo de los activos de información?					
7	¿Usted comunica oportunamente sobre las incidencias que se presentan en el manejo de los activos de información?					
8	¿Existe un procedimiento para el tratamiento especial a los incidentes de alto nivel de impacto?					
9	¿Se establecen controles de accesos al centro de datos?					
10	¿La institución invierte en nuevas tecnologías de información (servidores, PC, antivirus, licencias, etc.) con el fin de mantener mayor disponibilidad de los servicio de tecnología y seguridad de la información?					

Encuesta interna de usuarios finales para medir la gestión de riesgos asociados a los activos de información (hardware, software, base de datos, archivos) en la distribuidora local.

DATOS GENERALES:

Área: ……

Cargo: ……

Se ha diseñado el presente cuestionario con el objeto de tener un buen procedo de medición sobre la Gestión de Riesgos asociados a los activos de información, por lo que necesitamos de su colaboración. Marcar con una (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

Leyenda: 5. Siempre 4. Casi Siempre 3. A veces 2. Casi nunca 1. Nunca

	DIMENSIONES	ESCALA				
		1	2	3	4	5
	Cultura					
1	¿Ha recibido capacitación por parte del área de TI de cómo proteger su información?					
2	¿La institución ha implementado un plan de capacitación sobre gestión de riesgo en seguridad de la información?					
3	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información?					
	Recursos y Presupuesto					
4	¿Existe disponibilidad de los recursos (CPU, Impresoras, Muebles, antivirus etc.) que se usa para que los sistemas funcionen adecuadamente?					
5	¿Los recursos que Usted solicita para realizar sus actividades de trabajo son atendidos oportunamente.?					
6	¿Percibe que se asigna el suficiente personal técnico y de apoyo para el soporte de los sistemas.?					
	Infraestructura Tecnológica					
7	¿La institución cuenta con tecnología adecuada para el desarrollo de las actividades?					
8	¿La institución invierte en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para mantener mayor disponibilidad de los servicio de tecnología y seguridad de la información?					

9	¿Las computadoras asignadas para el desarrollo de sus actividades trabajan eficientemente y sin fallas?					
10	¿Cuenta con el servicio de internet adecuado, de acuerdo a las labores que realiza?					
11	¿Las computadoras están interconectadas a una red de corriente estabilizada?					
12	¿Las computadoras están interconectadas por una red para compartir de información.?					
	RRHH					
13	Conoce y utiliza métodos de seguridad de información para proteger la información.					
14	En cuanto a los problemas que se presentan con el Sistema no requiere asistencia técnica.					
15	Es natural navegar por internet y sabe cómo protegerse de virus y otros ataques.					
16	Es natural utilizar correo electrónico, y sabe cómo Protegerse de virus y otros ataques.					
17	Se considera usted un experto en el manejo de computadoras y sistemas.					

Anexo 2: Empresas encuestadas para el análisis del sector

1. **DISTRIBUIDORA "A" S.A.C**

   SECTOR: VENTA AL POR MAYOR DE MATERIALES DE CONSTRUCCIÓN, ARTÍCULOS DE FERRETERÍA Y EQUIPO Y MATERIALES DE FONTANERÍA Y CALEFACCIÓN.

   Misión: Poner al alcance de nuestros clientes una variedad de productos, dándoles un servicio personalizado y las mejores condiciones de calidad y precio.

   Visión: Ser una empresa con una fuerte presencia en diferentes regiones del Territorio Peruano, identificados por la excelencia en su servicio y ética en los negocios que emprende.

   Valores:

   ■ Honestidad ■ Trabajo en equipo ■ Respeto ■ Solidaridad ■ Justicia
   ■ Delegación ■ Integridad ■Servicios

   Estado del Encuestado: Participó en la encuesta.

2. **DISTRIBUIDORA "B" S.A.C**

   SECTOR: VENTA AL POR MAYOR DE MATERIALES DE CONSTRUCCIÓN, ARTÍCULOS DE FERRETERÍA Y EQUIPO Y MATERIALES DE FONTANERÍA Y CALEFACCIÓN.

   Misión: Somos una red de tiendas que comercializa materiales de construcción al mejor precio y con una buena calidad de servicio.

   Visión: Estamos trabajando para ser la mejor red de tiendas de materiales de construcción en el norte del Perú, basados en brindar productos de construcción y atención de la mejor calidad.

   Valores

   ■ Servicio ■ Calidad ■ Innovación ■ Responsabilidad

   Estado del Encuestado: Participó en la encuesta.

3. **DISTRIBUIDORA "C" S.A.**

SECTOR: COMERCIALIZACIÓN DE MATERIALES EMPLEADOS EN INSTALACIONES ELÉCTRICAS DE ALTA, MEDIA Y BAJA TENSIÓN (INDUSTRIALES Y DOMÉSTICAS).

Misión: Somos una empresa comercializadora de materiales eléctricos con un amplio stock de productos y ejecutora de obras y servicios electromecánicos.

Visión: Ser una empresa líder en la prestación de soluciones, ejecución de obras y servicios que satisfagan las expectativas de los clientes.

Valores

■ Servicio ■ Calidad ■ Responsabilidad

Estado del Encuestado: Participó en la encuesta.

4. **DISTRIBUIDORA S.A.C**

SECTOR: VENTA AL POR MAYOR DE MATERIALES DE CONSTRUCCIÓN, ARTÍCULOS DE FERRETERÍA Y EQUIPO Y MATERIALES DE FONTANERÍA Y CALEFACCIÓN

Misión: Somos una empresa creada para satisfacer el mercado de la construcción mediante la venta de Tuberías de PVC y Aditivos para la Construcción en infraestructura pública y privada, obras civiles, viales, urbanización.

Visión: Que La Casa del Aditivo sea el punto de referencia en todos los proyectos de construcción ofreciendo a nuestros clientes toda la gama de productos necesarios para la realización de su obra.

Valores

■ Trabajo en equipo ■Atención al cliente ■ Seguridad ■ Responsabilidad

Estado del Encuestado: Participó en la encuesta.

Anexo 3: Tabulación de resultados

Resultados de la encuesta de diagnóstico aplicada al personal líder del área de TI

Gráfico 01: COBIT5- APO12 Gestión del Riesgo: ¿En qué medida su organización considera el riesgo como parte del proceso de Planificación empresarial?

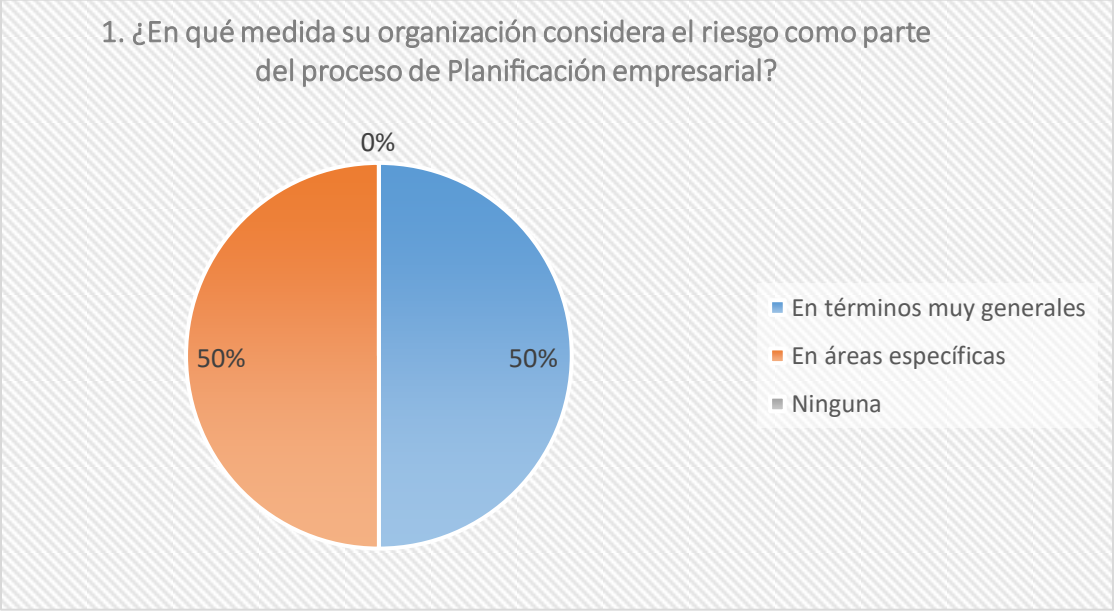


Gráfico 02: ¿En el organigrama de la Institución de quién depende el área de TI?

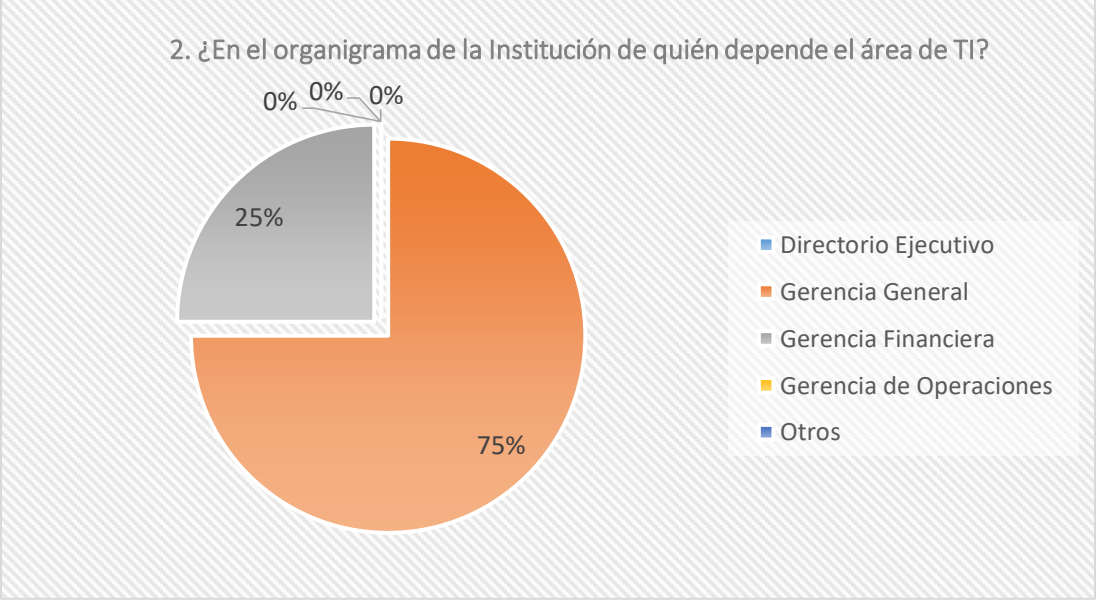


Gráfico 03: ¿Cuenta con un plan estratégico de TI?

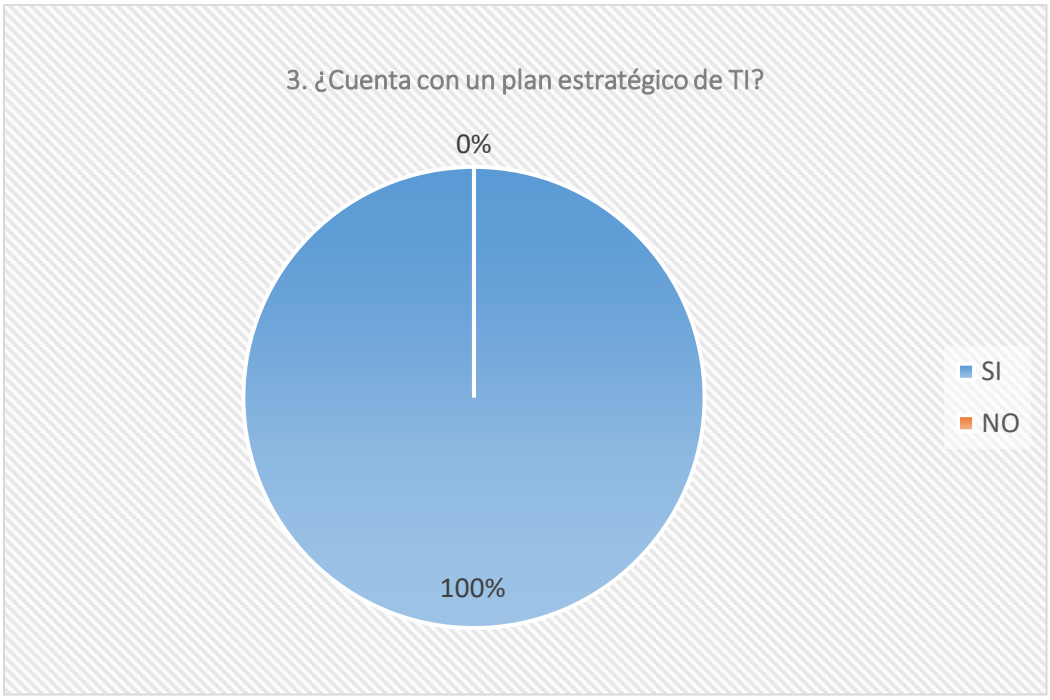


Gráfico 04: COBIT5- APO12.03 ¿Se ha realizado inventario de los activos de TI, incluyendo el personal de soporte, infraestructura, servicios, planes y registros de manuales críticos?

Gráfico 05: COBIT5-APO12 Metas de Gestión del Riesgo: ¿Los riesgos relacionados con los activos de TI están identificados, analizados, gestionados y reportados?

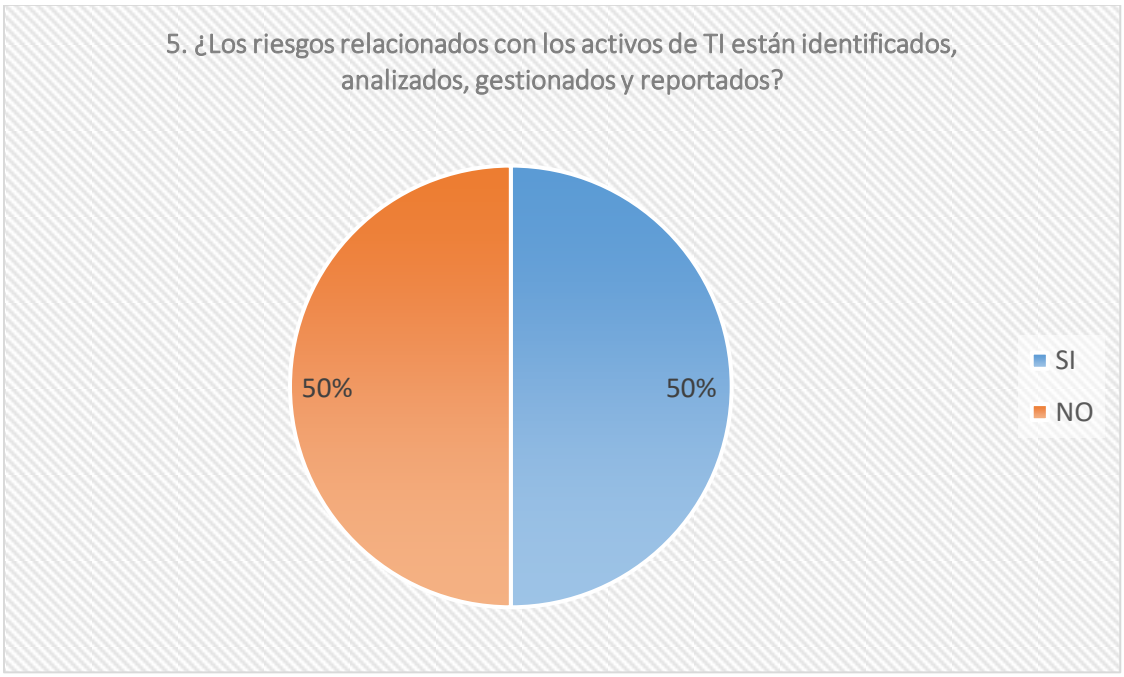


Gráfico 06: COBIT5-APO12.02: ¿La empresa ha estimado la pérdida económica asociada con escenarios de riesgo de TI que afectan a la disponibilidad del servicio?

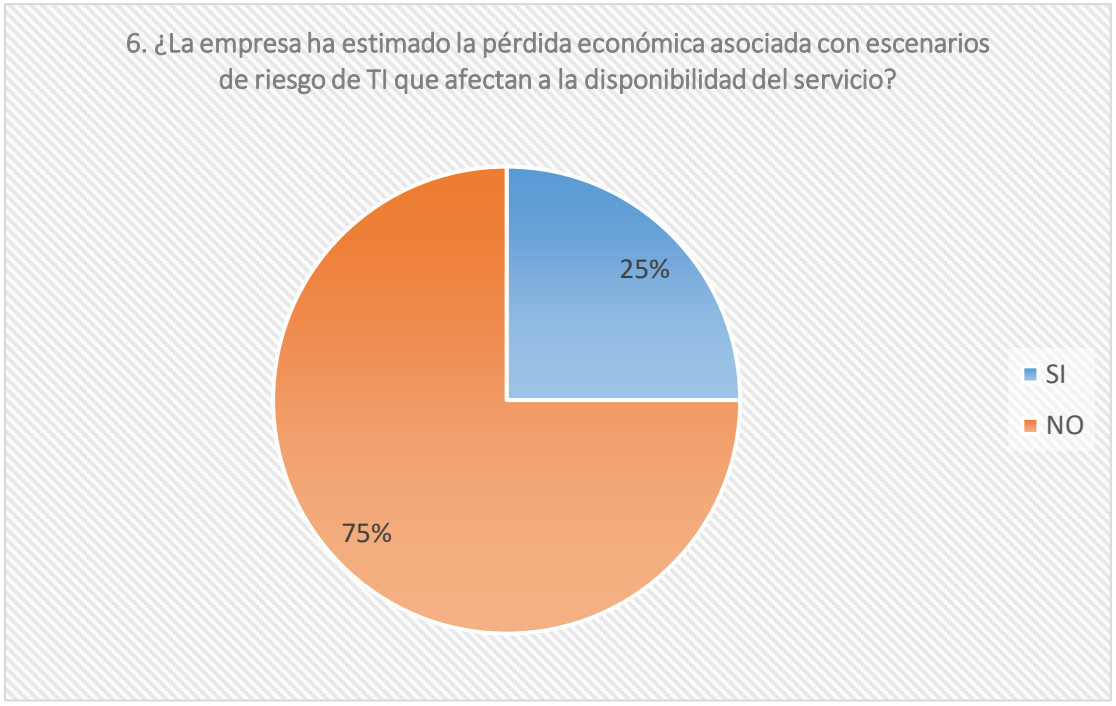


Gráfico 07: ¿El personal de TI posee las competencias y habilidades adecuadas para cumplir con su función?

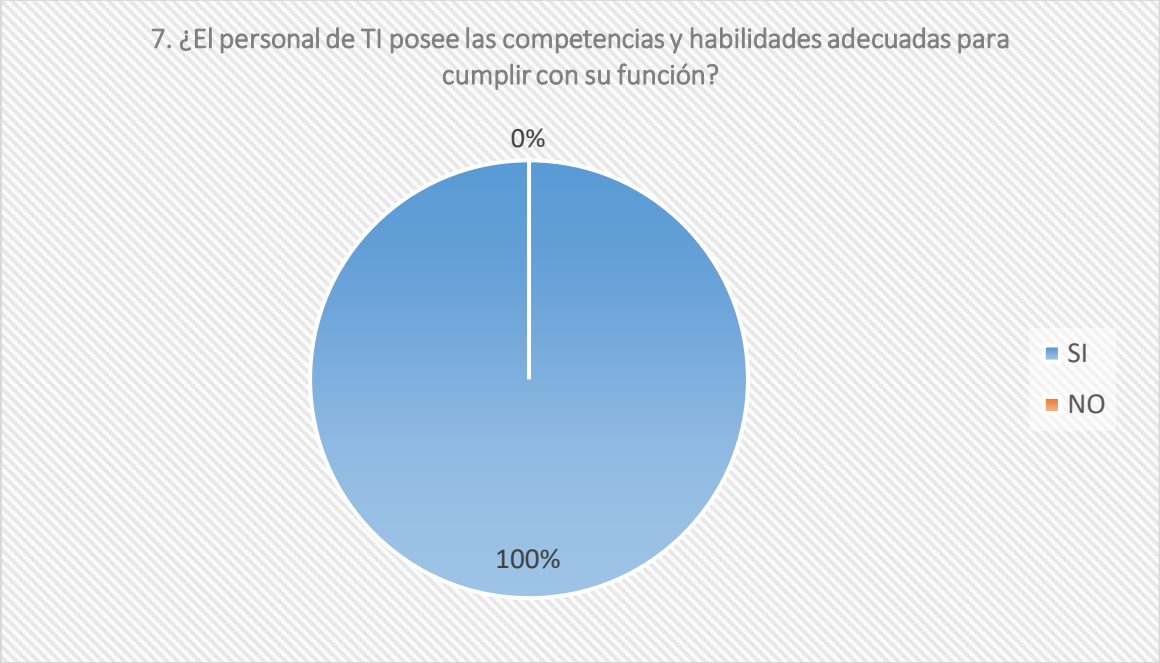


Gráfico 08: COBIT5- APO12.02 ¿Validan los resultados de análisis de riesgos antes de usarlos para la toma de decisiones de mitigación y respuesta al riesgo?

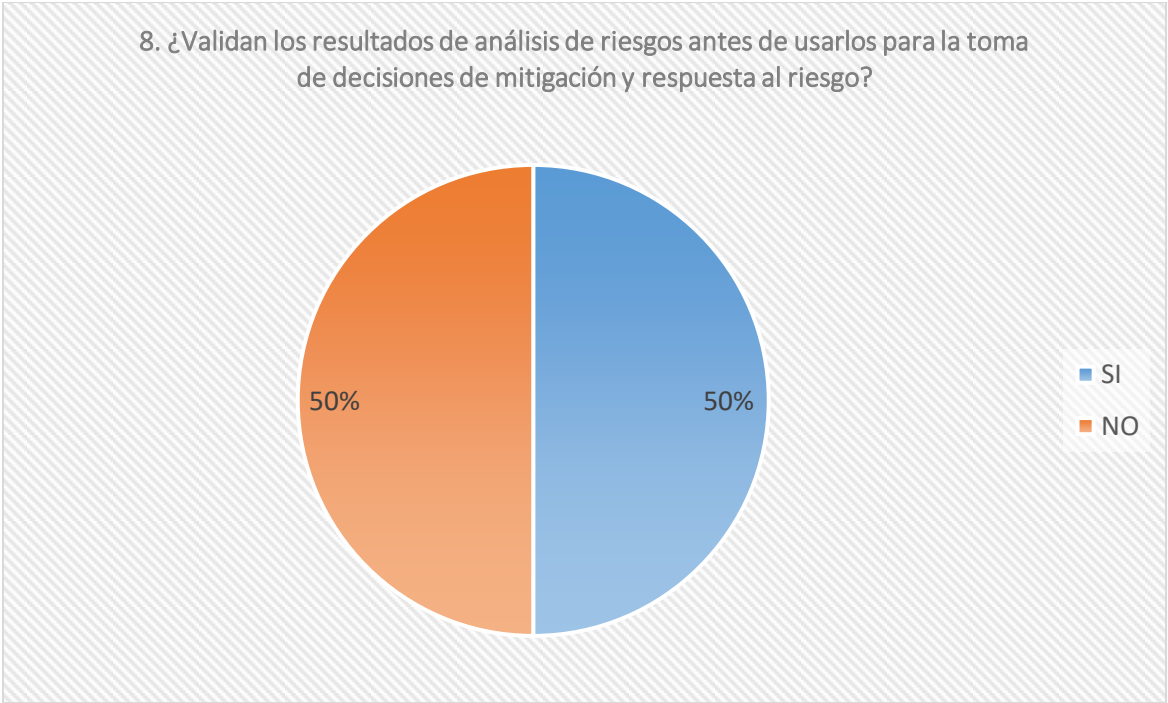


Gráfico 09: COBIT5-APO12.04 ¿Los riesgos de TI son informadas y coordinadas con la alta dirección de la empresa?

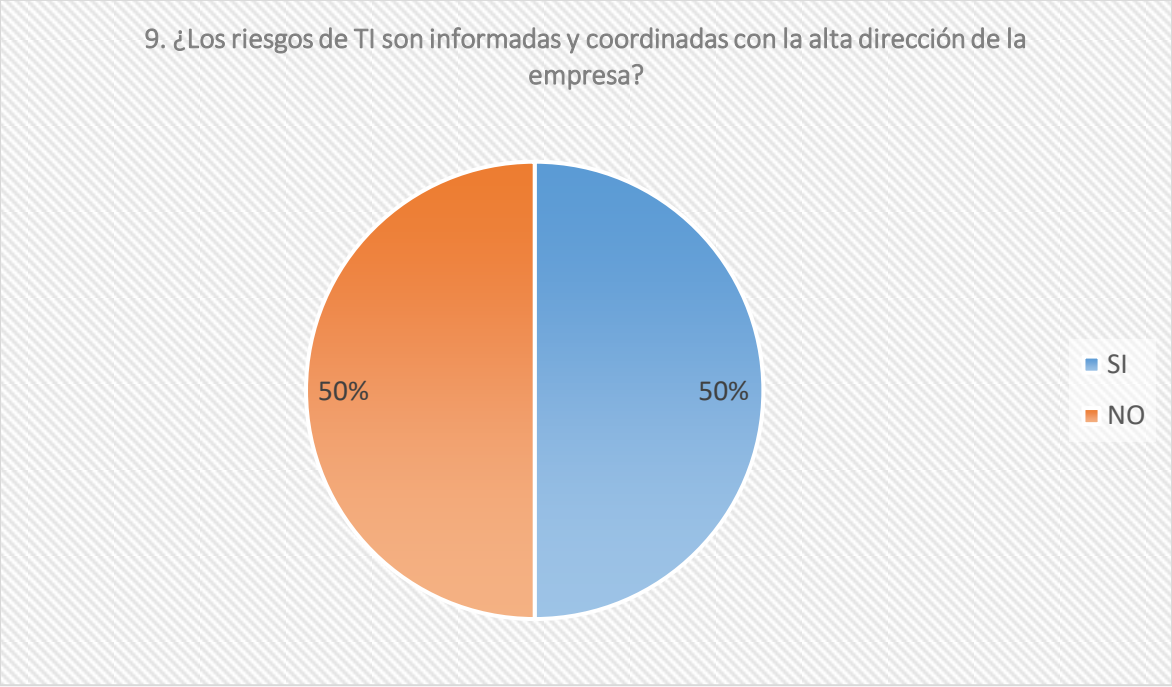


Gráfico 10: COBIT5- APO12.05 ¿La empresa ha determinado el nivel de riesgos relacionados con TI que está dispuesta a asumir para cumplir con sus objetivos?

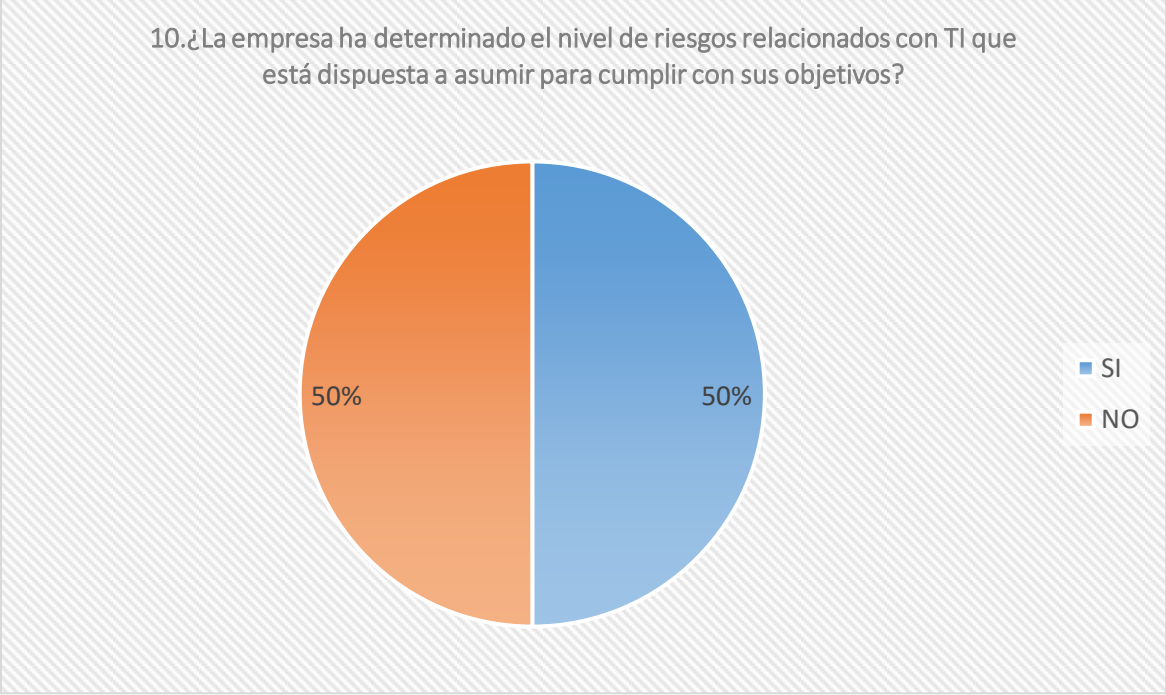


Gráfico 11: ¿Se ha determinado si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes?

Gráfico 12: COBIT5-APO12.06 ¿Se promueve una cultura consciente de los riesgos TI e impulsa a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio?

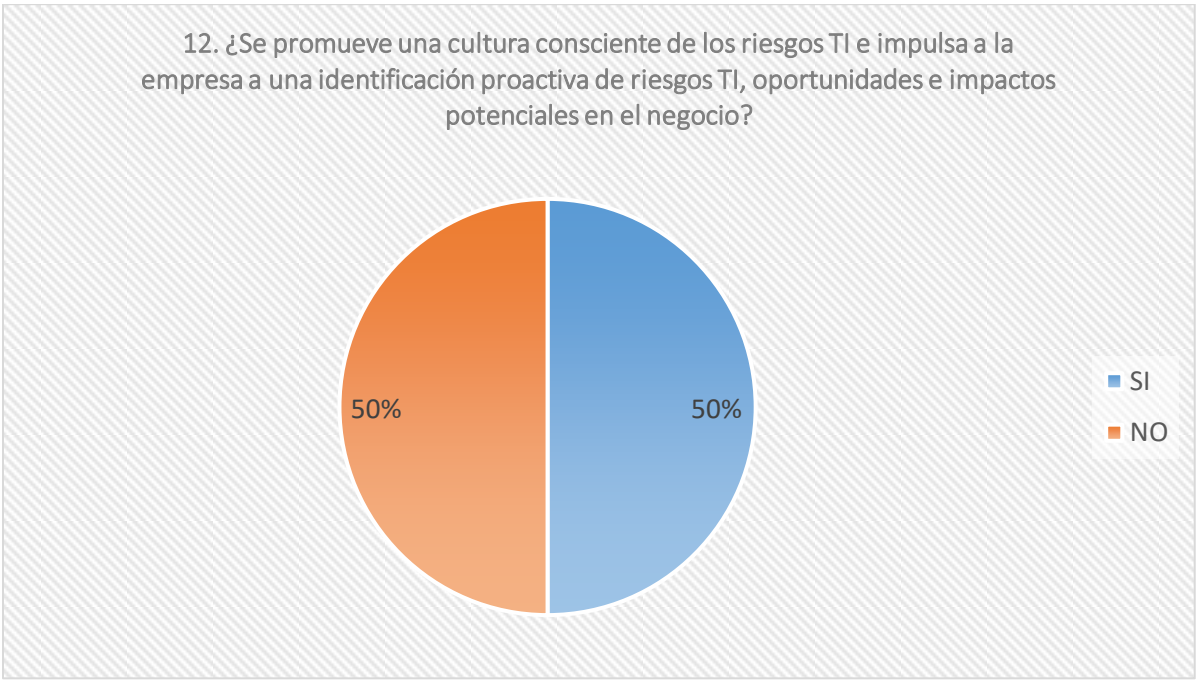


Gráfico 13: COBIT5-APO12.03 ¿Se ha identificado qué activos, servicios y recursos de TI son esenciales para sostener la operación de procesos de negocio, analizar dependencias y eslabones débiles?

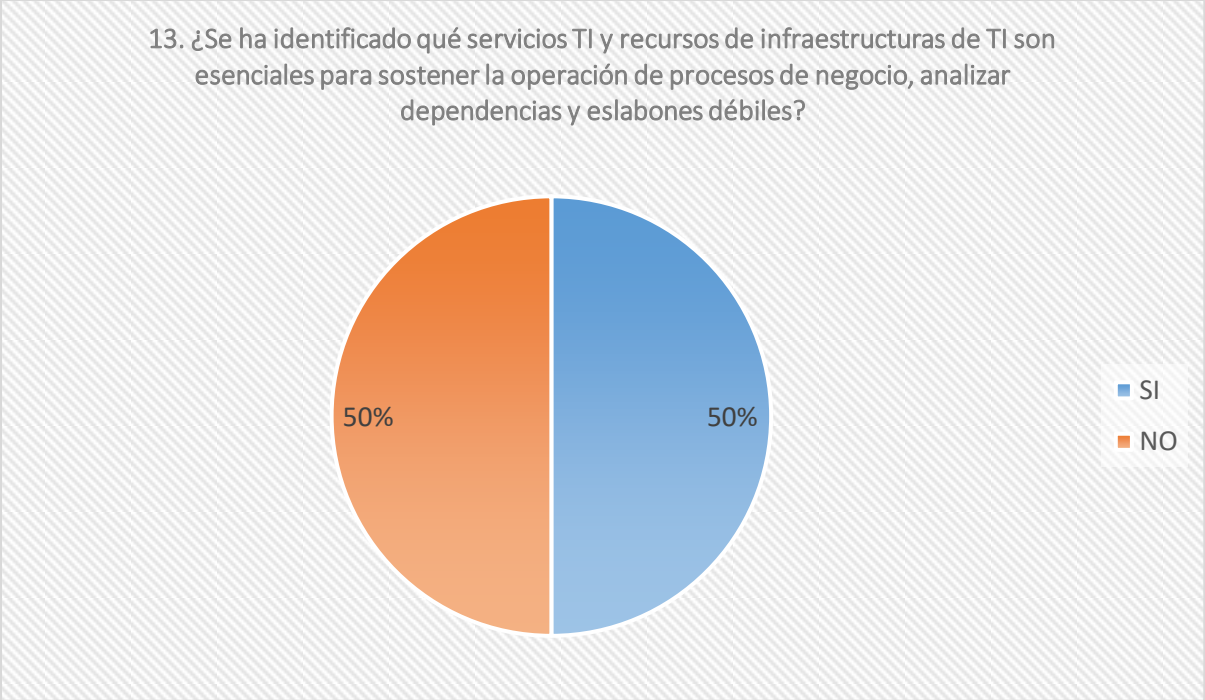


Gráfico 14: ¿El centro de datos y cuartos de comunicaciones cuentan con ambientes apropiados para su correcto funcionamiento? (aire acondicionado, área mínima, sistema de protección eléctrico, extintores, piso técnico, falso techo, etc.)

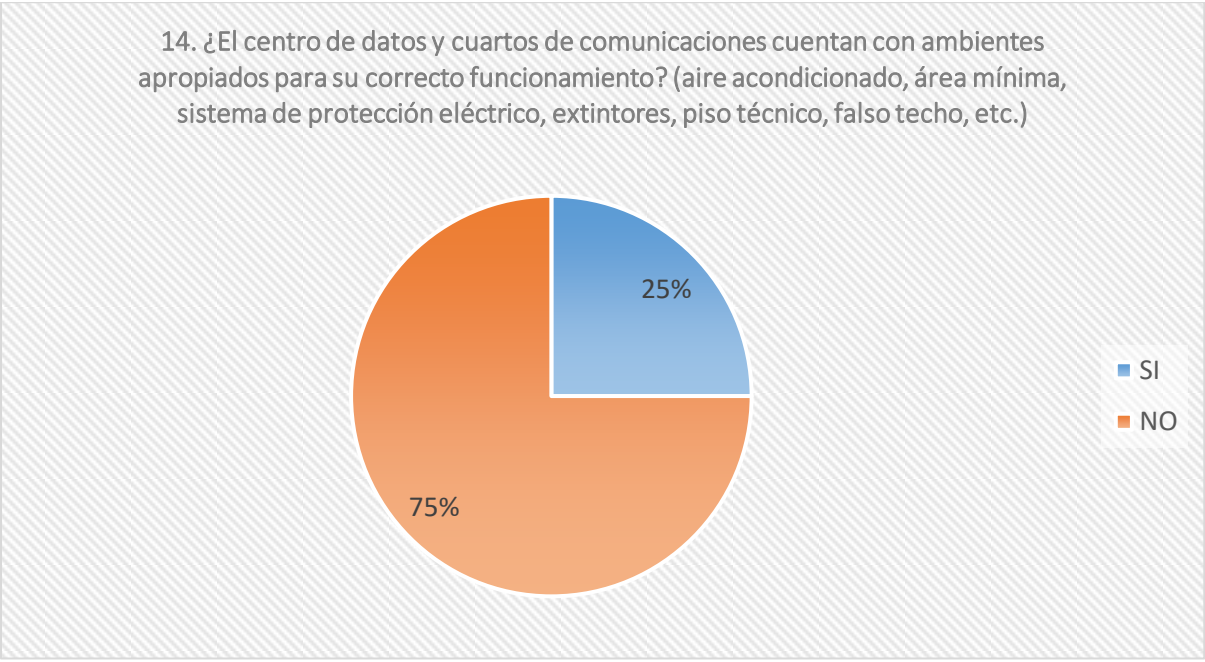


Gráfico 15: COBIT5-APO12.02 ¿Con que frecuencia se evalúa y actualiza los factores de riesgo de TI?

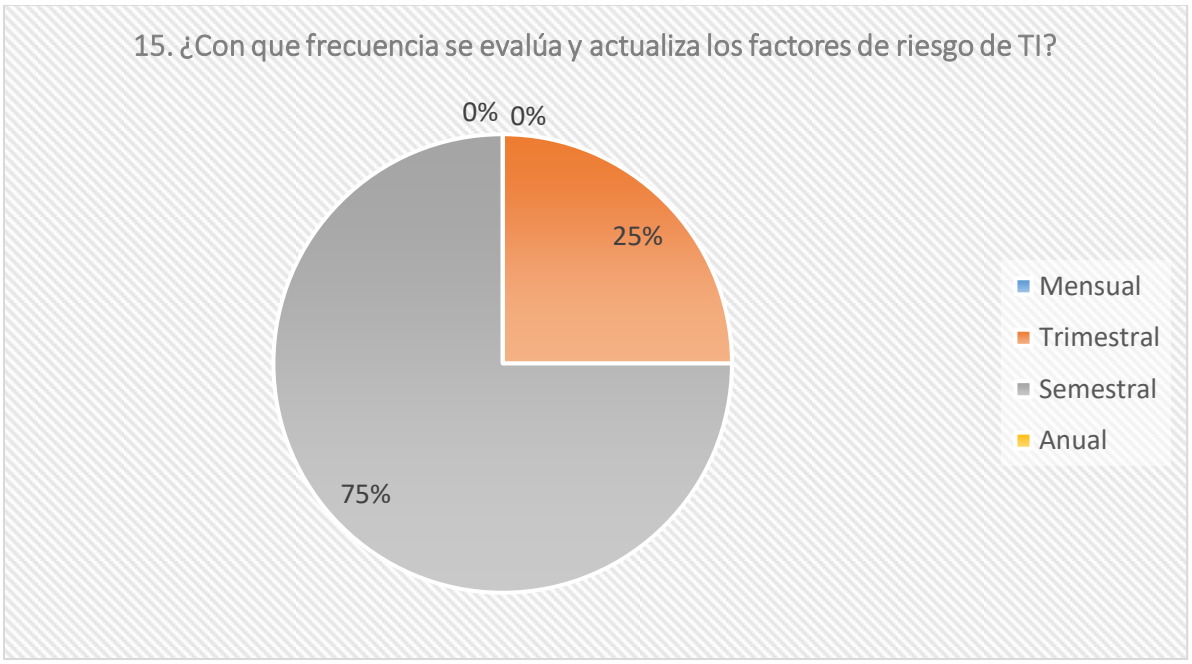
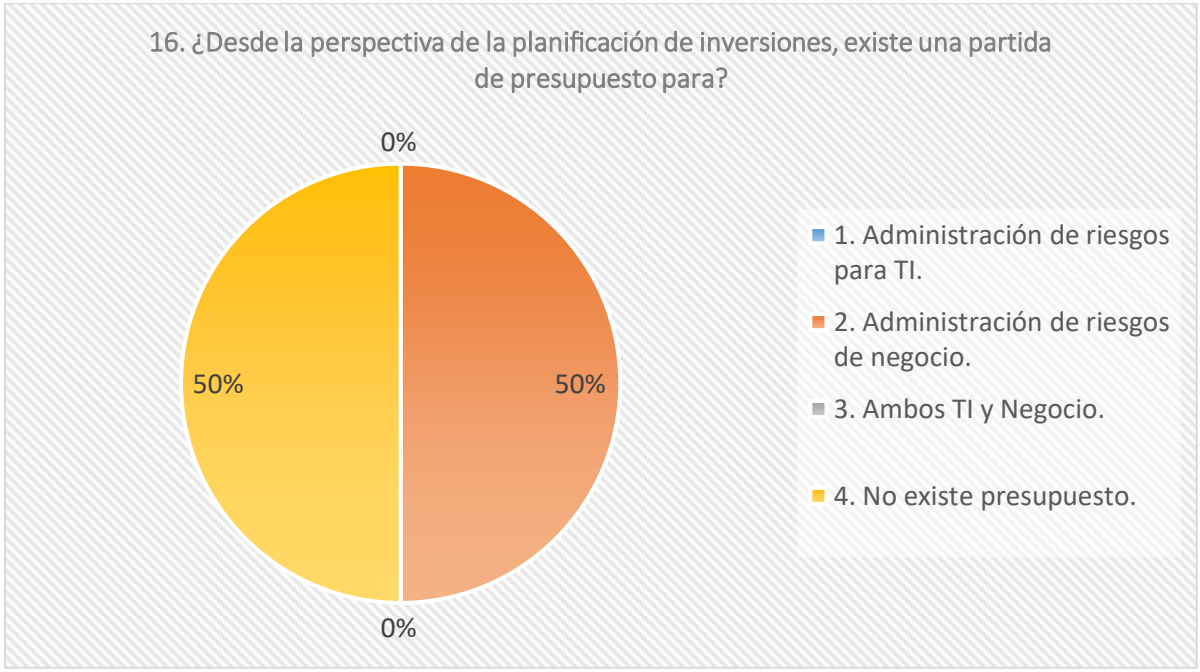


Gráfico 16: ¿Desde la perspectiva de la planificación de inversiones, existe una partida de presupuesto para?



Anexo 4: Implementación del modelo propuesto caso de aplicación empresa "Distribuidora A S.A.C"

Fase I: Alcance, contexto y criterio

1. Alcance

El objetivo del proyecto es realizar una identificación, análisis, y valoración de los riesgos que se encuentran inmersos los activos de TI, para tal fin se utiliza como elemento de soporte el análisis BIA que permite proveer una base especializada para identificar los proceso críticos de operación en la organización y estimar la afectación que podría padecer como resultado de la ocurrencia de un incidente.

Limitaciones: debido a la complejidad de realizar un análisis de todos los procesos y actividades del negocio en la distribuidora caso de estudio se trabajó en identificar los procesos más críticos a nivel operacional orientado a actividades de ventas y cumplimientos normativos contables, considerando también su relación u afectación a otros procesos.

Equipo de riesgos y responsabilidades:

- Directorio: personal de la empresa con nivel de autoridad (Gerente general, gerente adjunto, financiero, asesor legal) de establecer la prioridad de la gestión del riesgo a nivel operativo, financiero, estratégico y legal. Así mismo proporcionarán el soporte de definir el valor del apetito y tolerancia para cada evento de riesgo identificado.
- Dueño del proceso: personal de la empresa que propone los valores de prioridad de tiempos para recuperar el proceso transcurrido un incidente. Así mismo exigir el cumplimiento de la gestión del riesgo.
- Jefe de TI: personal de la empresa encargado de la identificación de los activos y la evaluación de sus riesgos probabilidad e impacto para el negocio, así mismo formulará planes de tratamiento para los riesgos identificados.

2. Establecimiento del contexto:

2.1 Contextos Internos

2.1.1 Cultural

MISIÓN

Poner al alcance de nuestros clientes una variedad de productos, dándoles un servicio personalizado y las mejores condiciones de calidad y precio.

VISIÓN

Ser una empresa con una fuerte presencia en diferentes regiones del Territorio Peruano, identificados por la excelencia en su servicio y ética en los negocios que emprende.

VALORES

- Honestidad
- Trabajo en equipo
- Respeto
- Solidaridad
- Justicia
- Delegación
- Integridad
- Servicio

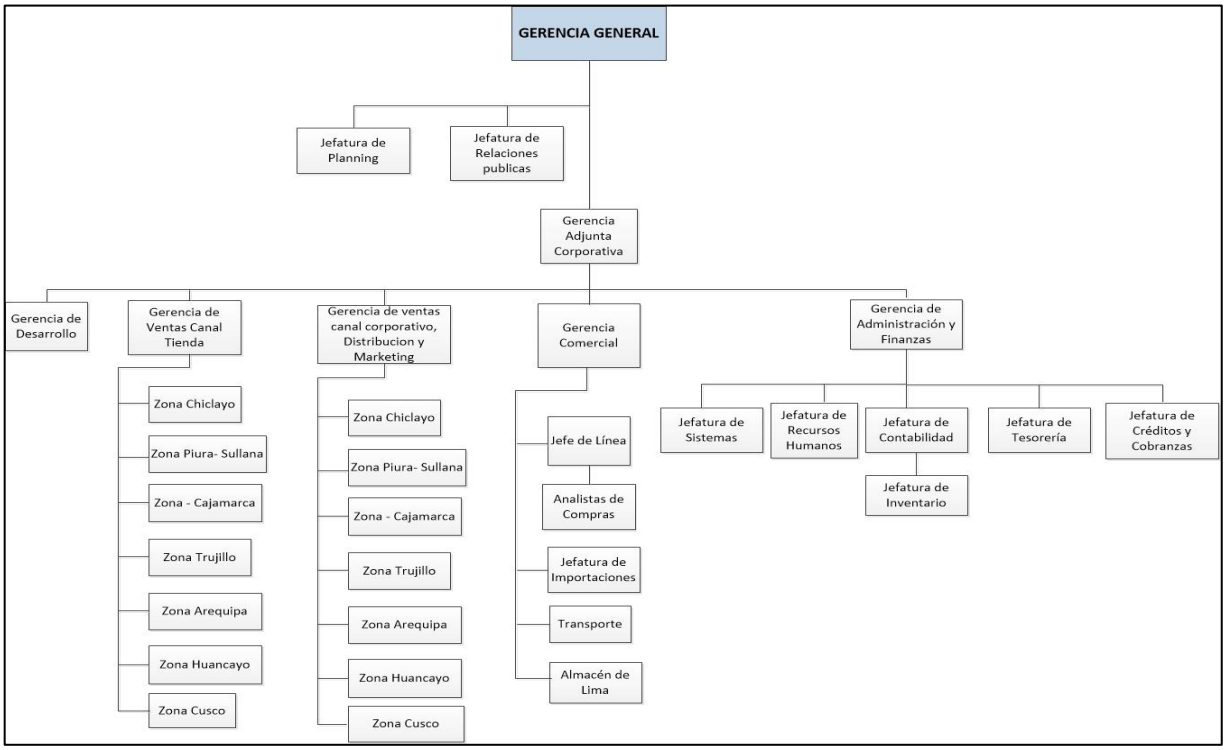
PARTES INTERESADAS

- Personal Administrativo (RRHH, Tesorería, Contabilidad, Sistemas, Inventarios, Cobranzas).
- Personal de operación de ventas.
- Personal Logístico Comercial.
- Personal de Dirección (Gerentes, Asesores).

2.1.2 Estructura Organizacional

La estructura de la organización es de tipo vertical con función colaborativa entre empleados y directivos que se agrupan por áreas, departamentos de acuerdo para gestionar su actividad y recursos. (Ver Organigrama corporativo).

Figura 11: Organigrama Corporativo Empresa Distribuidora A S.A.C



Fuente: Empresa Distribuidora A S.A.C

2.1.3 Recursos

Se define como el conjunto de activos tecnológicos que dan soporte a los procesos de la organización como sistemas de información, software de aplicación, servidores, equipos de cómputo, equipos de red, sistema de protección eléctrica, etc. El Inventario de infraestructura tecnológica será descrito en el punto de inventarios de activos.

2.1.4 Metas y Objetivos

Metas

- Calidad de Servicio: Capacitación constante al personal, optimización de procesos.
- Crecimiento en ventas.
- Expansión en el mercado: Abrir nuevas tiendas en el territorio nacional.

Objetivos institucionales:

- Fortalecer la organización basado en procesos de mejora continua.
- Alcanzar y mantener estratégicamente la excelencia operativa.
- Maximizar la rentabilidad de la Empresa.

2.2 Contextos Externos

2.2.1 Ámbito de Mercado

Elementos que tienen el potencial de afectar su economía y desempeño de la organización.

- Desarrollo económico en provincias.
- Niveles adquisitivos de clientes.
- Coste de productos importados.
- Costes de servicios de transporte.
- Crecimiento del sector retail en el Perú.

2.2.2 Ámbito Sociocultural

Relacionado a los grupos de interés como clientes con obras de construcción, constructoras, distribuidores ferreteros, gobiernos locales y otros organismos de la región.

- Mayor sofisticación de compra de clientes.
- Programas de capacitación.
- Integración clientes - empresa.

2.2.3 Ámbito Legal

Exigencias legales y reglamentarias, donde los riesgos de incumplimiento pueden poner en juego a la organización,

a) Operar conforme a la normativa fiscal.
   - La Superintendencia Nacional de Administración Tributaria (SUNAT).
   - Otras Legislaciones.

b) Para los negocios comerciales
   - Municipalidades (licencias municipales).
   - Instituto Nacional de Defensa Civil (INDECI).

c) Regulaciones laborales
   - Ministerio de Trabajo Promoción y Empleo (MTPE).

d) Tratado de libre comercio.
   - Ministerio de Economía y Finanzas (MEF).
   - La Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT).

2.2.4 Ámbito Económico

a) Estado económico del país.
b) Regulaciones de moneda extranjera.
c) SBS
d) BANCA
e) BCRP

2.2.5 Ámbito Tecnológico

Este ámbito está compuesto generalmente por factores que tienen que ver la rapidez de las innovaciones, el grado de desarrollo de tecnologías de información en organizaciones de distribuidoras.

- Infraestructura tecnológica sólida y redundante (Comunicación, infraestructura física y sistemas de información ERP: SAP, Net Suite, Microsoft Dynamics, etc.).
- Marketing digital (medios digitales: redes sociales, web, canal YouTube, etc.).
- Ventas Online (E-Commerce, MarketPlace)
- Estrategias de Omnicanalidad (comunicación fluida por medios digitales web, correo, aplicaciones móviles y tienda física).
- Análisis y explotación de la información (Analítica avanzada, Inteligencia de negocios).

3. Criterio

Para este punto la organización valora como criterio los siguientes riesgos en un grado porcentual que cederá a valorar el impacto para el negocio.

- Riesgos Operacionales (Peso 30%)
- Riesgos legales (Peso 25%)
- Riesgo económico (Peso 25%)
- Riesgo reputacional (Peso 20%)

Fase II: Análisis BIA

a. Priorización de procesos y actividades

En las siguientes tablas se realiza un listado de los procesos y actividades críticas e importantes para la organización siguiendo el criterio de valoración del impacto causado durante la ausencia de la actividad por franjas de horas,

EL CUADRO DE IDENTIFICACIÓN DE PROCESOS – EMPRESA DISTRIBUIDORA "A" S.A.C				
Num. Proceso	**CODIGO PROCESO**	**PROCESO**	**ÁREA O DEPARTAMENTO**	**DEPENDENCIA SERVICIOS DE TI**
1	[P_Venta]	Proceso de ventas.	Ventas	Módulo de gestión de ventas.
2	[P_Almacén]	Proceso de Almacén.	Ventas	Módulo de ingreso y despacho. Módulo de reparto de mercadería.
3	[P_Caja]	Proceso de cierre de caja.	Ventas	Módulo de planillas de cobranza.
4	[P_ Compras]	Proceso de Compras Nacionales.	Logística	Módulo de gestión de compras.
5	[P_ Importación]	Proceso de Compras Importadas.	Logística	Módulo de Importaciones.
6	[P_ PreciosCom]	Proceso de fijación de precios comerciales,	Logística	Módulo de lista de precios.
7	[P_ DistribuciónCD]	Proceso de distribución de productos a tiendas o almacenes.	Logística	Módulo de almacén central.
8	[P_Contabilidad]	Proceso de gestión contable.	Contabilidad	Módulo de contabilidad.
9	[P_Créditos]	Proceso de gestión de créditos.	Créditos y Cobranzas	Módulo de gestión de créditos y cobranzas.
10	[P_Inventario]	Proceso de gestión de inventario.	Inventarios	Módulo de gestión de inventarios.
11	[P_ Tesorería]	Proceso de gestión de tesorería.	Tesorería	Módulo de planillas de cobranza. Módulo de cuentas por pagar. Módulo de proceso de pagos RRHH. Módulo de bancos.
12	[P_GestiónRH]	Proceso de gestión Humana	Recursos Humanos	Módulo de RRHH
Fecha:01-05-2019		**Realizado Por: Wilson Cruz Cabrera**		**Aprobado Por: Gerencia General**

EL CUADRO DE ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA) – EMPRESA DISTRIBUIDORA "A" S.A.C													
COD. PROCESO	ACTIVIDAD	IMPACTOS ACUMULATIVOS POR HORAS DE INACTIVIDAD										CATEGORIA	CLASIFICACIÓN
		RTO (Horas)					RPO (Horas)						
		0-1	1-4	4-8	8-24	>24	0-1	1-4	4-8	8-24	>24		
[P_Ventas]	Consulta y registro de Cliente.	1	2	3	3	3	1	2	2	2	3	OPERACIONAL	MODERADO
	Generar cotización de productos.	2	3	4	4	4	2	2	2	3	3	OPERACIONAL	MAYOR
	Emitir comprobante de venta.	2	3	4	5	5	2	2	3	4	5	OPERATIVO	CATASTRÒFICO
	Genera ingreso de mercadería por devolución de cliente.	1	1	2	2	2	1	1	1	1	2	OPERACIONAL	MENOR
	Emite nota de crédito.	1	1	2	2	2	1	1	1	2	2	OPERACIONAL	MENOR
	Emite recibo de egreso.	1	1	1	2	2	1	1	1	2	2	OPERACIONAL	MENOR
	Enviar facturación por correo.	1	1	1	1	1	1	1	1	1	1	OPERACIONAL	INSIGNIFICANTE
[P_Almacén]	Registra ingresos de mercadería.	1	1	2	2	2	1	1	1	2	2	OPERACIONAL	MENOR
	Consulta ventas pendientes de despacho.	1	1	2	2	3	1	1	1	2	2	OPERACIONAL	MODERADO
	Genera despacho de mercadería.	1	1	2	2	3	1	1	1	2	2	OPERACIONAL	MODERADO
	Programación de reparto.	1	1	2	2	2	1	1	1	2	2	OPERACIONAL	MENOR
	Genera Guía de Remisión.	1	2	3	3	3	1	1	2	2	2	OPERACIONAL	MODERADO
[P_Caja]	Consulta e imprime reporte de ventas.	1	1	2	3	3	1	1	2	3	3	OPERACIONAL	MODERADO
	Registra depósitos a banco.	1	1	2	3	3	1	1	2	3	3	OPERACIONAL	MODERADO
	Consulta e imprime cobranza con tarjetas de crédito.	1	1	2	3	3	1	1	2	3	3	OPERACIONAL	MODERADO
	Genera liquidación de cobranza al contado.	1	1	2	3	3	1	1	2	3	3	OPERACIONAL	MODERADO
[P_ Compras]	Registro de padrón de ítems.	1	1	1	2	2	1	1	1	1	2	OPERATIVO	MENOR
	Análisis de necesidades de compra.	1	2	3	3	4	1	1	2	3	3	OPERACIONAL	MAYOR
	Genera órdenes de compra nacional.	2	2	3	3	4	1	1	2	3	4	OPERACIONAL	MAYOR
	Envío a proveedor.	2	2	3	3	4	1	1	2	3	4	OPERACIONAL	MAYOR
Fecha:01-05-2019		**Realizado Por: Wilson Cruz Cabrera**					**Aprobado Por: Gerencia General**						

EL CUADRO DE ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA) – EMPRESA DISTRIBUIDORA "A" S.A.C													
CODIGO PROCESO	ACTIVIDAD	IMPACTOS ACUMULATIVOS POR HORAS DE INACTIVIDAD										CATEGORIA	CLASIFICACIÓN
		RTO (Horas)					RPO (Horas)						
		0-1	1-4	4-8	8-24	>24	0-1	1-4	4-8	8-24	>24		
[P_Importación]	Registro de padrón de ítems.	1	1	1	1	1	1	1	1	1	1	OPERATIVO	INSIGNIFICANTE
	Evalúa requerimiento de Compra internacional.	1	1	2	2	2	1	1	1	2	2	OPERATIVO	MENOR
	Genera la orden de compra al exterior.	1	1	2	2	2	1	1	1	2	2	OPERATIVO	MENOR
	Registra factura de compra al exterior.	1	1	1	1	2	1	1	1	2	2	OPERATIVO	MENOR
	Genera página de embarque.	1	1	1	1	2	1	1	1	2	2	OPERATIVO	MENOR
	Genera la solicitud de distribución de productos importados.	1	1	2	2	2	1	1	1	2	2	OPERATIVO	MENOR
[P_ PreciosCom]	Actualizar precios de compra, descuento proveedor y fletes.	1	1	2	2	2	1	1	1	2	2	OPERATIVO	MENOR
	Actualizar precios de venta.	1	1	2	2	3	1	1	1	2	3	OPERATIVO	MODERADO
	Genera descuentos de venta.	1	1	2	3	3	1	1	2	3	3	OPERATIVO	MODERADO
[P_ DistribuciónCD]	Consulta requerimientos de reposición.	1	1	2	2	2	1	1	1	2	2	OPERATIVO	MENOR
	Genera transferencia entre establecimientos.	1	1	2	2	2	1	1	1	2	2	OPERATIVO	MENOR
[P_Contabilidad]	Registro de facturas de compras.	1	1	2	3	3	1	1	2	2	2	OPERATIVO	MODERADO
	Registro de gastos varios.	1	1	1	2	2	1	1	1	1	2	OPERATIVO	MENOR
	Generación de asientos diarios.	1	1	1	2	2	1	1	1	1	2	OPERATIVO	MENOR
	Declaración de libros electrónicos (de rentas e impuestos).	1	1	2	3	4	1	1	1	2	2	LEGAL	MAYOR
	Declaración de facturación electrónica.	2	2	3	3	4	1	1	2	2	3	LEGAL	MAYOR
Fecha:01-05-2019		**Realizado Por: Wilson Cruz Cabrera**					**Aprobado Por: Gerencia General**						

EL CUADRO DE ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA) – EMPRESA DISTRIBUIDORA "A" S.A.C													
CODIGO PROCESO	ACTIVIDAD	IMPACTOS ACUMULATIVOS POR HORAS DE INACTIVIDAD										CATEGORIA	CLASIFICACIÓN
		RTO (Horas)					RPO (Horas)						
		0-1	1-4	4-8	8-24	>24	0-1	1-4	4-8	8-24	>24		
[P_Créditos]	Análisis crediticio del cliente.	1	1	2	2	3	1	1	1	2	2	OPERATIVO	MODERADO
	Establecer línea de crédito.	1	1	2	2	3	1	1	1	2	2	OPERATIVO	MODERADO
	Consultar estados de cuenta por cobrar.	1	2	2	3	3	1	1	1	2	2	OPERATIVO	MODERADO
	Emitir cartas de cobranza.	1	1	2	2	2	1	1	1	2	2	OPERATIVO	MENOR
	Amortizar cobranza de venta al crédito.	1	1	2	2	2	1	1	1	2	2	OPERATIVO	MENOR
[P_Inventario]	Control de movimientos de entrada y salida.	1	1	1	2	2	1	1	1	2	2	OPERATIVO	MENOR
	Toma de Inventario.	1	1	1	2	2	1	1	1	2	2	OPERATIVO	MENOR
[P_Tesorería]	Análisis de cobranza de venta diaria por tienda.	1	1	2	3	3	1	1	1	2	2	OPERATIVO	MODERADO
	Cierre de ventas planilla diaria empresarial.	1	1	2	3	3	1	1	1	2	2	OPERATIVO	MODERADO
	Consulta cuentas por pagar proveedores.	1	1	2	3	3	1	1	2	2	3	OPERATIVO	MODERADO
	Generar pago a proveedores.	1	1	2	3	3	1	1	2	2	3	OPERATIVO	MODERADO
	Realizar pagos de haberes.	2	2	3	4	4	1	1	2	2	3	OPERATIVO	MAYOR
	Conciliación bancaria.	1	1	1	2	2	1	1	1	2	2	OPERATIVO	MENOR
[P_GestiónRH]	Generar contratos.	1	1	1	2	2	1	1	1	1	2	OPERATIVO	MENOR
	Procesamiento de asistencia.	1	1	1	2	2	1	1	1	1	2	OPERATIVO	MENOR
	Procesamiento de cálculo de remuneraciones.	1	1	2	3	3	1	1	1	2	2	OPERATIVO	MODERADO
	Programación de vacaciones.	1	1	1	2	2	1	1	1	1	2	OPERATIVO	MENOR
	Préstamos a personal.	1	1	1	2	2	1	1	1	1	2	OPERATIVO	MENOR
	Declaraciones PDT-Plame.	1	1	2	3	3	1	1	1	2	2	LEGAL	MODERADO
Fecha:01-05-2019		**Realizado Por: Wilson Cruz Cabrera**					**Aprobado Por: Gerencia General**						

En la presente matriz, se muestra un listado de procesos y actividades de la organización caso de estudio, que siguiendo los criterios de evaluación de los impacto descritos en la tabla Nª 3, nos permite expresar cual es el impacto durante la ausencia de la actividad para la organización por franjas de horas a fin de estimar el tiempo que se puede tolerar en el caso que un incidente o desastre le impida operar normalmente.

b. Análisis y consolidación

En el impacto operacional para la empresa caso de estudio se evidencia que está comprendido por los procesos core del negocio en su punto más crítico el procesos de ventas con afectación en su actividad de emitir comprobante de venta y generar cotización debido a que pueden convertirse en impactos económicos relevantes, así mismo los procesos compras nacionales y pagos de haberes se encuentran inmersos en un grado de impacto mayor, motivo que existen condiciones comerciales con proveedores que afectan a generar compras con anticipos de pago y pago diferido para su despacho, en cuanto a los pagos de haberes la empresa tiene el compromiso con sus colaboradores de muchos años historia del cumplimiento puntual en sus remuneraciones que el incurrir en el no cumplimiento genera un impacto interno que atente sobre la imagen de la empresa. Además en el proceso operativo se nota otros procesos y actividades de impacto moderados que dan soporte al ciclo comercial empresarial que se recomienda tener en cuenta.

En el impacto legal se evidencia que el proceso de contabilidad tiene dos actividades importantes en un grado de impacto mayor que se origina por la declaración de rentas e impuestos, declaración de documentos de venta electrónica que alcanzan poner en riesgo de sanciones legales tributarias con SUNAT por ser una empresa recaudadora de impuestos de retención tanto para con el proveedor y percepción para el cliente, así también el proceso de recursos humanos tiene las mismas obligaciones legales tributarias con las declaraciones del PDT y Plame.

Análisis y consolidación de procesos críticos			
Número proceso	**Proceso**	**Actividades por proceso**	**Actividades Priorizadas**
1	Proceso de ventas.	6	3
2	Proceso de Almacén.	5	2
3	Proceso de cierre de caja.	4	4
4	Proceso de compras nacionales.	3	3
5	Proceso de precios fijación de precios comerciales.	3	2
6	Proceso de gestión contable.	5	3

Análisis y consolidación de procesos críticos			
Número proceso	Proceso	Actividades por proceso	Actividades Priorizadas
7	Proceso de gestión de créditos.	5	3
8	Proceso de gestión de tesorería.	6	5
9	Proceso de gestión humana	6	2

Fase III: Evaluación del Riesgo

Para el desarrollo de esta fase la empresa por conocimiento informado, toma la decisión de iniciar la gestión de riesgos por su operación más crítica basada en ventas y acompañadas con las actividades legales de tributación contable que ponen en riesgo la operatividad comercial con el cliente.

3.1 Identificación de activos:

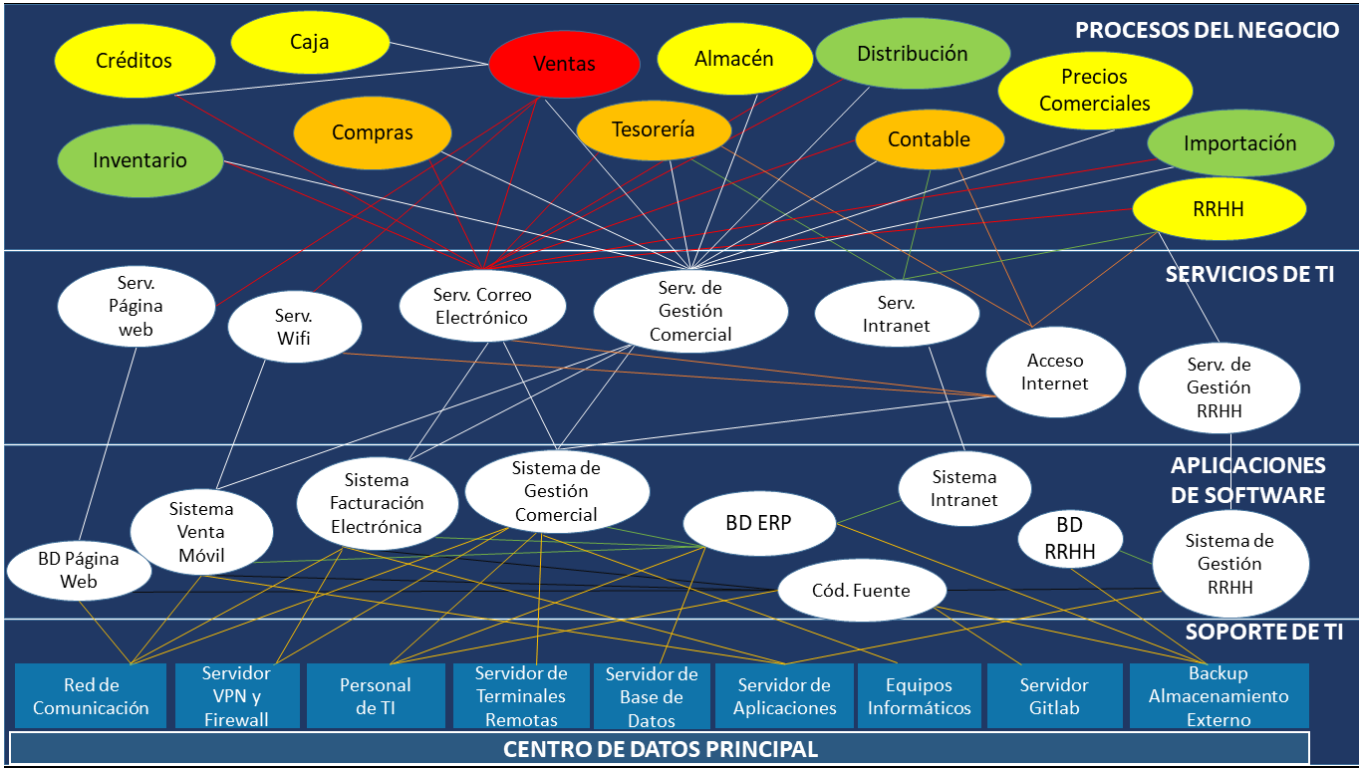
Listados de Tipos de activo de TI.		
Etiqueta	Tipo de Activo	Función
[ED]	Edificación e instalaciones físicas	Soporte
[HW]	Hardware (Equipamiento informático)	Soporte
[AP]	Aplicaciones (Software)	Aplicación
[COM]	Redes de comunicaciones.	Soporte
[MEDIA]	Medios de almacenamiento extraíble	Soporte
[IE]	Información electrónica	Datos
[IP]	Información en papel	Datos
[RH]	Recursos Humanos	Soporte
[S]	Servicios	Servicio
[P]	Procesos de negocio	Proceso

a) Clasificación de los activos

Registro de los activos de TI por tipo de activo				
Ítem	**Tipo de Activo**	**Activo de TI**	**Etiqueta Activo**	**Función**
1	[ED]	Centro de datos.	[ED_CDatos]	Soporte
2	[HW]	Servidor de aplicaciones	[HW_SrvApli]	Soporte
3	[HW]	Servidor de base de datos ERP	[HW_SrvBD]	Soporte
4	[HW]	Servidores de terminales remotas	[HW_SerTerm]	Soporte
5	[HW]	Servidor de VPN y Firewall	[HW_SerVpn]	Soporte
6	[HW]	Servidor de Gitlab	[HW_SerGit]	Soporte
7	[HW]	Equipos informáticos de usuario. (Computadoras de escritorio, laptop, impresoras, etc.)	[HW_EIU]	Soporte
8	[HW]	Equipos de comunicación (Switch Core, router, radio enlaces)	[HW_RedCom]	Soporte
9	[AP]	BD de sistema ERP	[AP_SBDErp]	Aplicación
10	[AP]	BD de sistema RRHH	[AP_SBDRrhh]	Aplicación
11	[AP]	BD Página web	[AP_SBDWeb]	Aplicación
12	[AP]	Sistema de gestión Comercial ERP	[AP_SCom]	Aplicación
13	[AP]	Sistema de facturación electrónica	[AP_SFE]	Aplicación
14	[AP]	Sistema de venta móvil	[AP_SVMov]	Aplicación
15	[AP]	Sistema de RRHH	[AP_SRRHH]	Aplicación
16	[AP]	Sistema de Intranet	[AP_SIntr]	Aplicación
17	[IE]	Códigos fuentes (Script, bibliotecas, etc.)	[IE_CodFuente]	Aplicación
18	[MEDIA]	Discos de almacenamiento externo (Backup de base de datos, de áreas, usuarios, manuales digitales)	[MED_DExt]	Soporte
19	[IP]	Documentos físicos (Reglamentos y procedimientos operacionales, planes, inventarios, contratos, etc.)	[IP_DocEmp]	Datos
20	[RH]	Personal de TI (De soporte, desarrollo y jefatura de TI)	[RH_PTI]	Soporte
21	[S]	Servicio de Gestión Comercial	[S_GesCom]	Servicio
22	[S]	Servicio página web	[S_PWeb]	Servicio
23	[S]	Servicio de intranet	[S_Intranet]	Servicio
24	[S]	Servicio de Wifi	[S_Wifi]	Servicio
25	[S]	Servicio de acceso a internet	[S_Internet]	Servicio
26	[S]	Servicio de correo electrónico	[S_EMail]	Servicio

b) Dependencias de los activos

Dependencia de activos.



Aplicando el enfoque bottom-up (de abajo arriba), se ha identificado los siguientes activos de TI que le dan soporte a los procesos de operación comercial.

c) Valoración de los activos

Confidencialidad (C)	Valor	Criterio
	5	Los daños serían catastróficos, la reputación y la imagen de la institución se verían comprometidas.
	4	Los daños serían relevantes, el incidente implica a otros procesos
	3	Daños bajos, el incidente no trasciende del proceso afectado.
	2	Daños muy bajos, el incidente no trasciende del proceso afectado.
	1	No aplica / No es relevante

Integridad (I)	Valor	Criterio
	5	Tiene que estar correcto y completo al menos en un 95.5%
	4	Tiene que estar correcto y completo al menos en un 75%
	3	Tiene que estar correcto y completo al menos en un 50%
	2	No es relevante los errores que tenga o la información que falte
	1	No aplica / No es relevante

Disponibilidad (D)	Valor	Criterio
	5	Debe estar disponible al menos el 95.5% del tiempo
	4	Debe estar disponible al menos el 75% del tiempo
	3	Debe estar disponible al menos el 50% del tiempo
	2	Debe estar disponible al menos el 10% del tiempo
	1	No aplica / No es relevante

Niveles de criticidad de los activos de TI			
Rango	Nivel de criticidad	Descripción	
1-3	1	Muy Bajo	MB
4-6	2	Bajo	B
7-9	3	Medio	M
10-12	4	Alto	A
13-15	5	Muy Alto	MA

CUADRO DE CRITERIOS DE CRITICIDAD DE ACTIVOS								
Etiqueta Categoría	Código Activo	N° Activo	Descripción	Criterios de Seguridad			Total	Nivel de Criticidad
				C	I	D		
[ED]	[ED_CDatos]	1	Centro de datos.	4	1	5	10	Alto [A]
[HW]	[HW_SrvApli]	2	Servidor de aplicaciones	4	4	5	13	Muy Alto [MA]
[HW]	[HW_SrvBD]	3	Servidor de base de datos ERP	5	5	5	15	Muy Alto [MA]
[HW]	[HW_SerTerm]	4	Servidores de terminales remotas	3	3	5	11	Alto [A]
[HW]	[HW_SerVpn]	5	Servidor de VPN y Firewall	2	4	4	10	Alto [A]
[HW]	[HW_SerGit]	6	Servidor de Gitlab	3	3	3	9	Medio [M]
[HW]	[HW_EIU]	7	Equipos de informáticos de usuario.	3	3	4	10	Alto [A]
[HW]	[HW_RedCom]	8	Equipos de comunicación	4	1	5	10	Alto [A]
[AP]	[AP_SBDErp]	9	BD de sistema ERP	5	5	5	15	Muy Alto [MA]
[AP]	[AP_SBDRrhh]	10	BD de sistema RRHH	3	5	4	12	Alto [A]
[AP]	[AP_SBDWeb]	11	BD Página web	3	3	4	10	Alto [A]
[AP]	[AP_SCom]	12	Sistema de gestión Comercial ERP	3	4	5	12	Muy Alto [MA]
[AP]	[AP_SFE]	13	Sistema de facturación electrónica	3	5	5	13	Muy Alto [MA]
[AP]	[AP_SVMov]	14	Sistema de venta móvil	3	5	4	12	Muy Alto [MA]
[AP]	[AP_SRRHH]	15	Sistema de RRHH	3	5	4	12	Alto [A]
[AP]	[AP_SIntr]	16	Sistema de Intranet	3	2	3	8	Medio [M]
[IE]	[IE_CodFuente]	17	Códigos fuentes	3	4	4	11	Alto [A]
[MEDIA]	[MED_DExt]	18	Discos de almacenamiento externo	5	5	5	15	Muy Alto [MA]
[IP]	[IP_DocEmp]	19	Documentos físicos	2	3	5	10	Alto [A]
[RH]	[RH_PTI]	20	Personal de TI	4	1	5	10	Alto [A]
[S]	[S_GesCom]	21	Servicio de Gestión Comercial	5	5	5	15	Muy Alto [MA]
[S]	[S_PWeb]	22	Servicio página Web corporativa	5	5	5	15	Muy Alto [MA]
[S]	[S_Intranet]	23	Servicio de Intranet	3	1	3	7	Medio [M]
[S]	[S_Wifi]	24	Servicio de Wifi	3	1	4	8	Medio [M]
[S]	[S_Internet]	25	Servicio de Acceso a Internet	4	1	5	10	Alto [M]
[S]	[S_EMail]	26	Servicio de Correo Electrónico	5	4	3	12	Alto [A]

3.2 Análisis del riesgo.

a) Identificar el riesgo

IDENTIFICIÓN DEL RIESGO						
Nro. de Activo	Código Activo	Activo	Amenaza	Vulnerabilidad	RIESGO	
					Código	Eventos / consecuencia de riesgo
1	[ED_CDatos]	Centro de datos.	Pertubación de la red eléctrica.	Inadecuado dimensionamiento y cableado de fluido eléctrico del DataCenter.	R1	Fallas eléctricas.
			Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico)	R2	Interrupción de las operaciones por energía eléctrica.
			Falla de equipos de climatización (aire acondicionado).	Inadecuado programa de mantenimiento de equipos del aire acondicionado.	R3	Sobrecalentamiento de equipos.
			Fuego (Incendio)	Carencia de sistema de seguridad, planes y procedimientos contra incendio.	R4	Pérdida de equipos por eventos de fuego.
			Agua (Inundaciones, fugas)	Cercanía a los ductos de ventilación, techos aligerados y suelo.	R5	Pérdida de equipos por agua.
			Desastres naturales.	Carencia de pólizas de seguro.	R6	Pérdida económica.
			Errores Humanos de operadores.	Carencia de buenas prácticas de operación y mantenimiento.	R7	Retraso de actividades por errores humanos.
			Acceso no autorizado.	Carencia de control de acceso de personal (Infraestructura física limitada).	R8	Robo o destrucción de equipos por acceso no autorizado.
			Obsolescencia tecnológica.	Falta de un plan de control de cambios de equipos según la vida útil y/o demanda operacional.	R9	Percepción negativa de los usuarios frente a la prestación de los servicios de TI.

IDENTIFICIÓN DEL RIESGO						
Nro. de Activo	Código Activo	Activo	Amenaza	Vulnerabilidad	RIESGO	
					Código	Eventos / consecuencia de riesgo
2	[HW_SrvApli]	Servidor de aplicaciones	Acceso no autorizado.	Falta de políticas de control de acceso y de auditoría.	R10	Fuga de información.
			Error de mantenimiento y actualización de software.	Inadecuado control de mantenimientos y actualización de software.	R11	Retraso en las operaciones,
				Intrusión de software malicioso.	R12	Pérdida de información por virus informáticos.
			Falla de acceso al servicio principal de internet.	Carencia de servicio de internet de respaldo.	R13	Pérdida de conexión de las sucursales a los sistemas de información.
			Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo.	R14	Interrupción de las operaciones de facturación.
3	[HW_SrvBD]	Servidor de base de datos ERP	Abuso de privilegios de acceso.	Falta de políticas de acceso al servidor de BD.	R15	Robo de información.
			Errores de mantenimiento y actualización de software.	Inadecuado control de mantenimientos y actualización de software.	R16	Retraso en las operaciones,
			Error de configuración de hardware.	Carencia de un plan de gestión de cambios.	R17	Fallas de operación del equipo.
			Agotamiento de recursos de hardware.	Inadecuado dimensionamiento de hardware (disco duro, memoria ram, etc.,)	R18	Interrupción del sistema y lentitud de las operaciones.
			Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico)	R19	Interrupción de las operaciones por corte de energía eléctrica.

IDENTIFICIÓN DEL RIESGO						
Nro. de Activo	Código Activo	Activo	Amenaza	Vulnerabilidad	RIESGO	
					Código	Eventos / consecuencia de riesgo
4	[HW_SerTerm]	Servidores de terminales remotas.	Denegación de acceso al servicio.	Carencia de licenciamiento y soporte del servicio RDP.	R20	Intrusión de virus y control no autorizado al equipo.
			Falla de acceso al servicio principal de internet.	Carencia de servicio de internet de respaldo.	R21	Pérdida del servicio por conexión de internet.
			Abuso de privilegios de acceso.	Falta de políticas de control de acceso y de auditoría.	R22	Robo de información.
			Errores de mantenimiento y actualización de software.	Inadecuado control de mantenimientos y actualización de software.	R23	Retraso en las operaciones,
			Agotamiento de recursos de hardware.	Inadecuado dimensionamiento de hardware (disco duro, memoria ram, etc.,)	R24	Interrupción del sistema y lentitud de las operaciones.
			Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico)	R25	Interrupción de las operaciones de facturación.
5	[HW_SerVpn]	Servidor de VPN y Firewall	Denegación de servicios.	Carencia de un sistema de información de administración de eventos y monitoreo de red (log).	R26	Pérdida del servicio por evento de denegación de servicios.
			Falla de acceso al servicio principal de internet.	Carencia de servicio de internet de respaldo.	R27	Pérdida del servicio por conexión de internet.
			Error de mantenimiento y actualización de software.	Inadecuado control de mantenimientos y actualización de software.	R28	Retrasos en las operaciones.
			Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico)	R29	Interrupción de las operaciones de facturación y compras por corte de energía eléctrica.

IDENTIFICIÓN DEL RIESGO						
Nro. de Activo	Código Activo	Activo	Amenaza	Vulnerabilidad	RIESGO	
					Código	Eventos / consecuencia de riesgo
7	[HW_EIU]	Equipos de informáticos de usuario (computadoras de escritorio, laptop, impresoras, etc.)	Obsolescencia tecnológica de equipos de cómputo.	Carencia de un plan de cambios de equipos de cómputo de acuerdo a su vida útil.	R30	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo.
			Avería de software.	Carencia de licencias de software de sistema operativo.	R31	Sanciones legales y económicas.
				Inadecuado control de actualización de software.	R32	Retrasos en las operaciones.
				Intrusión de software malicioso.	R33	Robo y pérdida de información por virus informáticos.
			Avería de hardware.	Carencia de procedimientos adecuados de copia de seguridad.	R34	Pérdida de información por fallas de hardware.
				Incumplimiento del plan de mantenimiento de equipos (hardware).	R35	Degradación de la vida útil del equipo.
				Carencia de un plan de seguridad física.	R36	Pérdida del equipo por daños de hardware.
			Hurto de equipos	Deficiencia de procedimientos de control de salida e ingresos de equipos.	R37	Pérdida del equipo por robo.
			Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico)	R38	Interrupción de las operaciones por corte de energía eléctrica.
			Fuego (Incendio)	Carencia de sistema de seguridad contra incendio, planes y procedimientos contra incendio.	R39	Pérdida de equipos por eventos de fuego.
			Agua (Inundaciones, fugas)	Infraestructura inadecuada para instalación de equipos.	R40	Pérdida de equipos por eventos de agua.
			Desastres naturales.	Carencia de pólizas de seguro.	R41	Pérdida económica.

IDENTIFICIÓN DEL RIESGO						
Nro. de Activo	Código Activo	Activo	Amenaza	Vulnerabilidad	RIESGO	
					Código	Eventos / consecuencia de riesgo
8	[HW_RedCom]	Equipos de comunicación (Switch, router, radio enlaces)	Avería de equipos de comunicación	Falla del Switch core	R42	Pérdida de la conexión la red LAN
				Falla de equipos de radios enlaces	R43	Pérdida de la conexión de la red MAN
				Falla de equipos de enrutamiento WAN	R44	Pérdida de la conexión de la red WAN.
				Ausencia de políticas de mantenimiento preventivo de los equipos de comunicación.	R45	Deterioro del equipo e infraestructura de comunicación.
			Corte de energía eléctrica.	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico)	R46	Inoperatividad de los equipos de comunicaciones y de acceso. Desconexión de la red.
			Fuego (Incendio)	Carencia de sistema de seguridad, planes y procedimientos contra incendio.	R47	Pérdida de equipos por eventos de fuego.
			Agua (Inundaciones, fugas)	Infraestructura inadecuada para instalación de equipos.	R48	Pérdida de equipos por agua.
			Desastres naturales.	Carencia de pólizas de seguro.	R49	Pérdida económica.
9	[AP_SBDErp]	BD de sistema ERP	Abuso de privilegios de acceso.	Falta de procedimientos de validación de consultas.	R50	Pérdida e inconsistencia de datos por manipulación intencional o accidental.
				Carencia de auditoría detallada acciones ejecutadas a la base de datos.	R51	Fuga de información.
			Indisponibilidad del personal DBA	Dependencia excesiva del personal que gestiona la Base de Datos.	R52	Retraso de operación.
11	[AP_SBDWeb]	BD página web	Acceso no autorizado.	Modificación no autorizada de BD y configuraciones.	R53	Pérdida de integridad de datos
				Carencia de auditoría detallada de acceso y acciones ejecutadas a la base de datos.	R54	Robo de información.

IDENTIFICIÓN DEL RIESGO						
Nro. de Activo	Código Activo	Activo	Amenaza	Vulnerabilidad	RIESGO	
					Código	Eventos / consecuencia de riesgo
12	[AP_SCom]	Sistema de gestión Comercial ERP	Errores de mantenimiento / actualización de software.	Carencia de documentación técnica.	R55	Errores de configuración.
				Carencia de un plan de actualización de software.	R56	Retraso en la actualización de software.
				Compatibilidad del ERP (sistemas operativos y versión de aplicaciones de ofimática).	R57	Retraso en las operaciones.
			Errores de programación y validación.	Carencia de buenas prácticas de programación. (Inyección SQL, entrada de datos.)	R58	Manipulación no autorizada y pérdida de integridad de datos.
				Deficiencia en el diseño de base datos (normalización de BD).	R59	Pérdida de rendimiento y eficiencia del sistema.
			Caída del sistema por sobrecarga de transacciones	Carencia de un sistema de información y procedimientos para administración de eventos.	R60	Bloqueo de operaciones transaccionales.
			Indisponibilidad de soporte proveedor.	Ausencia de contractos comerciales y de acuerdos de SLA.	R61	Retraso en la atención de requerimientos.
			Abuso de privilegios de acceso.	Ausencia de Workflow por proceso de negocio.	R62	Fuga de información.
13	[AP_SFE]	Sistema de facturación electrónica	Errores de mantenimiento / actualización de software	Carencia de un plan de actualización de software.	R63	Retraso en la actualización de software.
			Caída del sistema por sobrecarga de transacciones.	Carencia de un sistema de información para administración de eventos.	R64	Bloqueo de operaciones transaccionales.
			Abuso de privilegios de acceso.	Ausencia de políticas de perfiles de acceso descritos y autorizados.	R65	Fuga de información.

IDENTIFICIÓN DEL RIESGO						
Nro. de Activo	Código Activo	Activo	AMENAZA	VULNERABILIDAD	RIESGO	
					Código	Eventos / consecuencia de riesgo
14	[AP_SVMov]	Sistema de venta móvil	Errores de mantenimiento / actualización de software	Carencia de un plan de actualización de software.	R66	Retraso en la actualización de software.
			Caída del sistema por sobrecarga de transacciones.	Carencia de un sistema de información para administración de eventos.	R67	Bloqueo de operaciones transaccionales.
			Abuso de privilegios de acceso.	Ausencia de políticas de perfiles de acceso a la información.	R68	Fuga de información.
18	[MED_DExt]	Discos de almacenamiento externo (Backup)	Avería de tipo físico	Carencia de procedimientos adecuados de copia de seguridad y almacenamiento de los medios externos.	R69	Deterioro del dispositivo de almacenamiento.
			Avería de tipo lógico	Intrusión de software malicioso en medios de almacenamiento externo.	R70	Corrupción de archivos (datos).
			Abuso de privilegios de acceso.	Carencia de procedimientos de utilización de medios de almacenamiento externos.	R71	Robo y fuga de información.
21	[S_GesCom]	Servicio de Gestión Comercial	Abuso de privilegios de acceso.	Ausencia de políticas de perfiles de acceso descritos y autorizados.	R72	Robo y fuga de información.
			Indisponibilidad del administrador del sistema.	Inadecuado programa de capacitación al personal.	R73	Falta de formación adecuada del personal.
			Indisponibilidad del administrador del sistema.	Dependencia excesiva del administrador del software.	R74	Retraso en las operaciones.

IDENTIFICIÓN DEL RIESGO						
Nro. de Activo	Código Activo	Activo	AMENAZA	VULNERABILIDAD	RIESGO	
					Código	Eventos / consecuencia de riesgo
22	[S_PWeb]	Servicio página Web corporativa	Error de usuario.	Carencia de validación de datos entradas del usuario.	R75	Pérdida de integridad de datos
			Acceso no Autorizado.	Carencia de un sistema de información para administración de eventos.	R76	Robo y alteración de la información.
			Indisponibilidad del administrador de TI	Dependencia excesiva del administrador de la página web	R77	Retraso en las publicaciones de operación web.
24	[S_Wifi]	Servicio de Wifi	Uso no previsto	Ausencia de políticas de uso del servicio.	R78	Saturación del servicio.
			Acceso no Autorizado	Ausencia de controles de acceso a usuarios.	R79	Robo de información
25	[S_Internet]	Servicio de Acceso a Internet	Falla de acceso al servicio principal de internet.	Carencia de acceso a internet de respaldo	R80	Interrupción servicio de Internet y conexión a los sistemas de información.
			Uso no previsto	Carencia de un servidor de firewall especializado a nivel de hardware y software para monitoreo de la red.	R81	Saturación del servicio y fuga de información.
26	[S_EMail]	Servicio de Correo Electrónico	Falla de acceso al servicio principal de internet.	Carencia de acceso a internet de respaldo	R82	Interrupción del servicio.
			Falla del archivo de correo del usuario	Ausencia de políticas de mantenimiento de cliente de correo.	R83	Pérdida de información de correo.
			El aumento de la necesidades de ancho de banda y almacenamiento	Ausencia de políticas de uso del correo.	R84	Saturación del servicio de internet.
			Difusión de software dañino	Ausencia de políticas de seguridad y capacitación al usuario.	R85	Robo de información u suplantación de identidad.

Del análisis realizado en los cuadros de identificación de riesgos, se tiene como resultado un total de 85 riesgos detectados en los activos de TI, riesgos que se distribuyen en 9 de edificación e instalaciones físicas (R1-R9), 32 de hardware informático (R10-R41), 8 de redes de comunicación (R42-49), 19 de aplicaciones de software (R50-R68), 3 medios de almacenamiento extraíble (R69-R71) y 14 de servicios (R72-R85).

b) Determinar probabilidad e impacto

Valoración de los niveles de Probabilidad		
Nivel	Probabilidad	Descripción
1	Raro	No se presenta en varios años.
2	Improbable	Se podría presentar una vez al año.
3	Posible	Se podría presentar hasta tres veces al año.
4	Probable	Se podría presentar mensualmente.
5	Casi Seguro	Se podría presentar a diario.

Valoración de los niveles de Impactos		
Nivel	Impacto	Descripción
1	Muy Bajo	Tiene un efecto adverso insignificante en las operaciones o activos de la organización.
2	Bajo	Tiene un efecto adverso limitado en las operaciones o activos, de la organización.
3	Medio	Tiene un efecto adverso considerable que ralentiza operaciones o activos de la organización.
4	Alto	Tiene un efecto adverso grave o catastrófico que paraliza algunas operaciones o activos críticos de la organización.
5	Muy alto	Tiene un efecto adverso grave o catastrófico que paraliza todas las operaciones o activos críticos de la organización.

3.3 Valoración de los activos

a) Valorar el Riesgo

TABLA DE CATEGORÍA DEL RIESGO	
NIVEL DE RIESGO	**CALIFICACIÓN**
MUY ALTO	**15 A 25**
ALTO	9 A 14
MEDIO	4 A 8
BAJO	1 A 3

Para establecer la tabla categoría del riesgo se optó por realizar una matriz de calor tomando como referencia su valorización en función de los criterios de probabilidad e impacto con la siguiente fórmula: Riesgo= Probabilidad x Impacto

VALORIZACIÓN DE PROBABILIDAD POR IMPACTO DE LAS AMENAZAS						
PROBABILIDAD	VALOR	1	2	3	4	5
CASI SEGURO	5	5	10	15	20	25
PROBABLE	4	4	8	12	16	20
POSIBLE	3	3	6	9	12	15
IMPROBABLE	2	2	4	6	8	10
RARO	1	1	2	3	4	5
	IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO

CUADRO DE VALORIZACIÓN DEL RIESGO						
Código	PROBABILIDAD		IMPACTO		Evaluación Del Riesgo	Categoría
	Nivel	Descripción	Nivel	Descripción		
R1	2	Improbable	3	Medio	6	Medio
R2	3	Posible	5	Muy Alto	15	Muy Alto
R3	2	Improbable	2	Bajo	4	Medio
R4	1	Raro	5	Muy Alto	5	Medio
R5	2	Improbable	3	Medio	6	Medio
R6	1	Raro	5	Muy Alto	5	Medio
R7	3	Posible	2	Bajo	6	Medio
R8	4	Probable	4	Alto	16	Muy Alto
R9	2	Improbable	3	Medio	6	Medio
R10	3	Posible	3	Medio	9	Alto
R11	2	Improbable	3	Medio	6	Medio
R12	1	Raro	3	Medio	3	Bajo
R13	3	Posible	4	Alto	12	Alto
R14	2	Improbable	4	Alto	8	Medio
R15	4	Probable	4	Alto	16	Muy Alto
R16	2	Improbable	5	Muy Alto	10	Alto
R17	1	Raro	5	Muy Alto	5	Medio
R18	1	Raro	4	Alto	4	Medio
R19	2	Improbable	5	Muy Alto	10	Alto
R20	1	Raro	4	Alto	4	Medio
R21	3	Posible	4	Alto	12	Alto
R22	4	Probable	3	Medio	12	Alto
R23	2	Improbable	4	Alto	8	Medio
R24	2	Improbable	4	Alto	8	Medio
R25	2	Improbable	5	Muy Alto	10	Alto
R26	2	Improbable	4	Alto	8	Medio

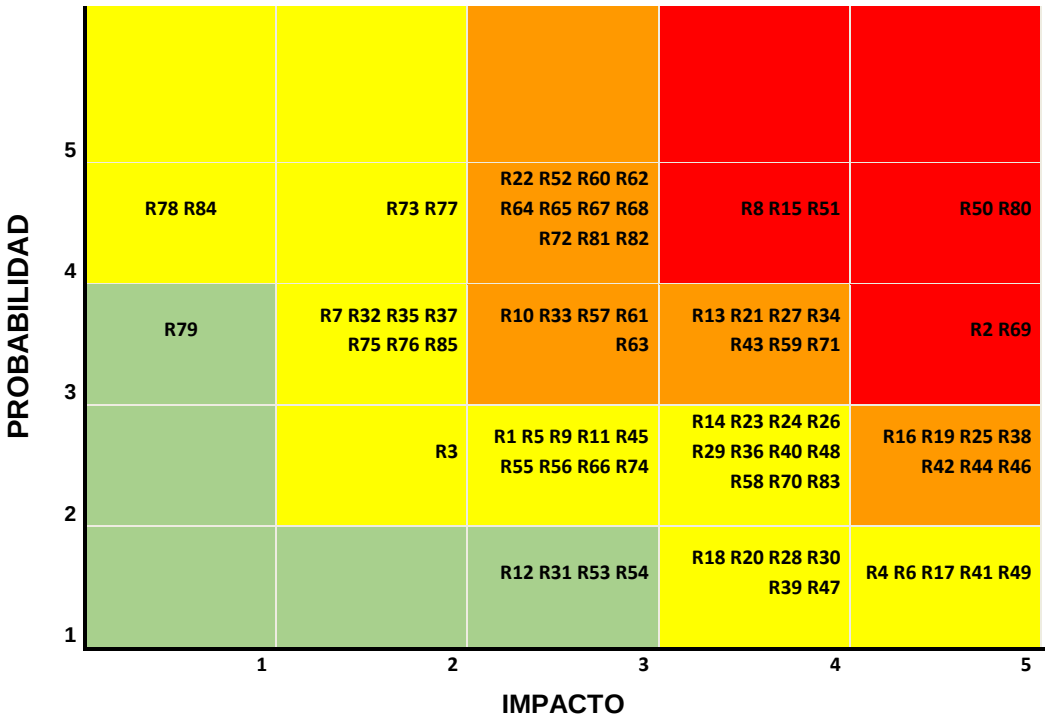
CUADRO DE VALORIZACIÓN DEL RIESGO						
Código	PROBABILIDAD		IMPACTO		Evaluación Del Riesgo	Categoría
	Nivel	Descripción	Nivel	Descripción		
R27	3	Posible	4	Alto	12	Alto
R28	1	Raro	4	Alto	4	Medio
R29	2	Improbable	4	Alto	8	Medio
R30	1	Raro	4	Alto	4	Medio
R31	1	Raro	3	Medio	3	Bajo
R32	3	Posible	2	Bajo	6	Medio
R33	3	Posible	3	Medio	9	Alto
R34	3	Posible	4	Alto	12	Alto
R35	3	Posible	2	Bajo	6	Medio
R36	2	Improbable	4	Alto	8	Medio
R37	3	Posible	2	Bajo	6	Medio
R38	2	Improbable	5	Muy Alto	10	Alto
R39	1	Raro	4	Alto	4	Medio
R40	2	Improbable	4	Alto	8	Medio
R41	1	Raro	5	Muy Alto	5	Medio
R42	2	Improbable	5	Muy Alto	10	Alto
R43	3	Posible	4	Alto	12	Alto
R44	2	Improbable	5	Muy Alto	10	Alto
R45	2	Improbable	3	Medio	6	Medio
R46	2	Improbable	5	Muy Alto	10	Alto
R47	1	Raro	4	Alto	4	Medio
R48	2	Improbable	4	Alto	8	Medio
R49	1	Raro	5	Muy Alto	5	Medio
R50	4	Probable	5	Muy Alto	20	Muy Alto
R51	4	Probable	4	Alto	16	Muy Alto
R52	4	Probable	3	Medio	12	Alto
R53	1	Raro	3	Medio	3	Bajo
R54	1	Raro	3	Medio	3	Bajo
R55	2	Improbable	3	Medio	6	Medio
R56	3	Posible	3	Medio	9	Alto
R57	3	Posible	3	Medio	9	Alto
R58	2	Improbable	4	Alto	8	Medio
R59	3	Posible	4	Alto	12	Alto
R60	4	Probable	3	Medio	12	Alto
R61	3	Posible	3	Medio	9	Alto
R62	4	Probable	3	Medio	12	Alto

CUADRO DE VALORIZACIÓN DEL RIESGO						
Código	PROBABILIDAD		IMPACTO		Evaluación Del Riesgo	Categoría
	Nivel	Descripción	Nivel	Descripción		
R63	3	Posible	3	Medio	9	Alto
R64	4	Probable	3	Medio	12	Alto
R65	4	Probable	3	Medio	12	Alto
R66	2	Improbable	3	Medio	6	Medio
R67	4	Probable	3	Medio	12	Alto
R68	4	Probable	3	Medio	12	Alto
R69	3	Posible	5	Muy Alto	15	Muy Alto
R70	2	Improbable	4	Alto	8	Medio
R71	3	Posible	4	Alto	12	Alto
R72	4	Probable	3	Medio	12	Alto
R73	4	Probable	2	Bajo	8	Medio
R74	2	Improbable	3	Medio	6	Medio
R75	3	Posible	2	Bajo	6	Medio
R76	3	Posible	2	Bajo	6	Medio
R77	4	Probable	2	Bajo	8	Medio
R78	4	Probable	1	Medio	4	Medio
R79	3	Posible	1	Medio	3	Bajo
R80	4	Probable	5	Muy Alto	20	Muy Alto
R81	4	Probable	3	Medio	12	Alto
R82	4	Probable	3	Medio	12	Alto
R83	2	Improbable	4	Alto	8	Medio
R84	4	Probable	1	Muy Bajo	4	Medio
R85	3	Posible	2	Bajo	6	Medio

Del análisis realizado en los cuadros de valorización del riesgo tomando como base la probabilidad de frecuencia por el impacto para la organización caso de estudio, el resultado obtenido es 7 riesgos caracterizados como Muy Alto, 31 con categoría Alto, 42 con categoría Medio y 5 riesgos como Bajos (para ver el detalle de la nomenclatura R1 al R85 ubicarse en el cuadro de identificación de riesgos).

b) Priorizar el riesgo

Matriz de priorización de riesgos.



En la presente matriz de priorización de riesgo se representa gráficamente el impacto cuantitativo y cualitativo de los riesgos detectados en la fase de evaluación del riesgo a fin de facilitar la toma de decisiones en la organización caso de estudio. Como podemos observar la información resultante de los cuadros de valoración del riesgo son ubicadas en el mapa de calor donde eje x representa la probabilidad de frecuencia del riesgo y el eje y representa el impacto que puede tener el mismo.

MATRIZ DE PRIORIZACIÓN Y CONTROL DE RIESGOS									
RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R80	Muy Alto	[S_Internet]	Servicio de Acceso a Internet	Falla de acceso al servicio principal de internet.	Carencia de acceso a internet de respaldo	20	6	9	Debe ser tratado
R50	Muy Alto	[AP_SBDErp]	BD de sistema ERP	Abuso de privilegios de acceso.	Falta de procedimientos de validación de consultas.	20	4	8	Debe ser tratado
R15	Muy Alto	[HW_SrvBD]	Servidor de base de datos ERP	Abuso de privilegios de acceso.	Falta de políticas de acceso al servidor de BD.	16	4	8	Debe ser tratado
R8	Muy Alto	[ED_CDatos]	Centro de datos.	Acceso no autorizado.	Carencia de control de acceso de personal (Infraestructura física limitada).	16	3	6	Debe ser tratado
R51	Muy Alto	[AP_SBDErp]	BD de sistema ERP	Abuso de privilegios de acceso.	Carencia de auditoría detallada acciones ejecutadas a la base de datos.	16	4	8	Debe ser tratado
R2	Muy Alto	[ED_CDatos]	Centro de datos.	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (Generador eléctrico, UPS)	15	6	8	Debe ser tratado
R69	Muy Alto	[MED_DExt]	Discos de almacenamiento externo	Avería de tipo físico	Carencia de procedimientos adecuados de copia de seguridad y almacenamiento de los medios externos.	15	4	6	Debe ser tratado
R13	Alto	[HW_SrvApli]	Servidor de aplicaciones	Falla de los servicios de comunicación.	Carencia de servicio de internet de respaldo.	12	6	9	Debe ser tratado
R21	Alto	[HW_SerTerm]	Servidores de terminales remotas	Falla de los servicios de comunicación.	Carencia de servicio de internet de respaldo.	12	6	9	Debe ser tratado
R27	Alto	[HW_SerVpn]	Servidor de VPN y Firewall	Falla de los servicios de comunicación	Carencia de servicio de internet de respaldo.	12	6	9	Debe ser tratado
R22	Alto	[HW_SerTerm]	Servidores de terminales remotas	Abuso de privilegios de acceso.	Falta de políticas de control de acceso y de auditoría.	12	6	12	Tolerable
R34	Alto	[HW_EIU]	Equipos de informáticos de usuario	Avería de hardware	Carencia de procedimientos adecuados de copia de seguridad.	12	6	9	Debe ser tratado

MATRIZ DE PRIORIZACIÓN Y CONTROL DE RIESGOS									
RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R43	Alto	[HW_RedCom]	Equipos de comunicación	Avería de equipos de comunicación.	Falla de equipos de radios enlaces	12	6	16	Tolerable
R52	Alto	[AP_SBDErp]	BD de sistema ERP	Indisponibilidad del personal DBA	Dependencia excesiva del personal que gestiona la Base de Datos.	12	8	12	Tolerable
R59	Alto	[AP_SCom]	Sistema de gestión Comercial ERP	Errores de programación y validación.	Deficiencia en el diseño de base datos (normalización de BD).	12	4	6	Debe ser tratado
R60	Alto	[AP_SCom]	Sistema de gestión Comercial ERP	Caída del sistema por sobrecarga de transacciones	Carencia de un sistema de información y procedimientos para administración de eventos.	12	9	12	Tolerable
R62	Alto	[AP_SCom]	Sistema de gestión Comercial ERP	Abuso de privilegios de acceso.	Ausencia de Workflow por proceso de negocio.	12	3	6	Debe ser tratado
R64	Alto	[AP_SFE]	Sistema de facturación electrónica	Caída del sistema por sobrecarga de transacciones.	Carencia de un sistema de información para administración de eventos.	12	9	12	Tolerable
R65	Alto	[AP_SFE]	Sistema de facturación electrónica	Abuso de privilegios de acceso.	Ausencia de políticas de perfiles de acceso descritos y autorizados.	12	8	12	Tolerable
R67	Alto	[AP_SVMov]	Sistema de venta móvil	Caída del sistema por sobrecarga de transacciones.	Carencia de un sistema de información para administración de eventos.	12	9	12	Tolerable
R68	Alto	[AP_SVMov]	Sistema de venta móvil	Abuso de privilegios de acceso.	Ausencia de políticas de perfiles de acceso a la información.	12	8	12	Tolerable
R71	Alto	[MED_DExt]	Discos de almacenamiento externo	Abuso de privilegios de acceso.	Carencia de procedimientos de utilización de medios de almacenamiento externos.	12	9	12	Tolerable

MATRIZ DE PRIORIZACIÓN Y CONTROL DE RIESGOS									
RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R72	Alto	[S_GesCom]I	Servicio de Gestión Comercial	Abuso de Privilegios	Ausencia de políticas de perfiles de acceso descritos y autorizados.	12	8	12	Tolerable
R81	Alto	[S_Internet]	Servicio de Acceso a Internet	Uso no previsto	Carencia de un servidor de firewall especializado a nivel de hardware y software para monitoreo de la red.	12	3	6	Debe ser tratado
R82	Alto	[S_EMail]	Servicio de Correo Electrónico	Falla de acceso al servicio de internet.	Carencia de acceso a internet de respaldo	12	6	12	Tolerable
R16	Alto	[HW_SrvBD]	Servidor de base de datos ERP	Errores de mantenimiento y actualización de software.	Inadecuado control de mantenimientos y actualización de software.	10	6	10	Tolerable
R19	Alto	[HW_SrvBD]	Servidor de base de datos ERP	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (Generador eléctrico, UPS)	10	4	6	Debe ser tratado
R25	Alto	[HW_SerTerm]	Servidores de terminales remotas	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (Generador eléctrico, UPS)	10	4	6	Debe ser tratado
R38	Alto	[HW_EIU]	Equipos de informáticos de usuario	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (Generador eléctrico)	10	6	12	Tolerable
R42	Alto	[HW_RedCom]	Equipos de comunicación	Avería de equipos de comunicación.	Falla del Switch core	10	5	10	Tolerable
R44	Alto	[HW_RedCom]	Equipos de comunicación	Avería de equipos de comunicación.	Falla de equipos de enrutamiento WAN	10	8	10	Tolerable
R46	Alto	[HW_RedCom]	Equipos de comunicación	Corte de energía eléctrica.	Falta de abastecimiento de energía eléctrica de respaldo (Generador eléctrico, UPS)	10	4	6	Debe ser tratado
R10	Alto	[HW_SrvApli]	Servidor de aplicaciones	Acceso no autorizado.	Falta de políticas de control de acceso y de auditoría.	9	12	16	Tolerable

MATRIZ DE PRIORIZACIÓN Y CONTROL DE RIESGOS									
RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R33	Alto	[HW_EIU]	Equipos de informáticos de usuario	Avería de software	Intrusión de software malicioso.	9	6	12	Tolerable
R56	Alto	[AP_SCom]	Sistema de gestión Comercial ERP	Errores de mantenimiento / actualización de software.	Carencia de un plan de actualización de software.	9	6	12	Tolerable
R57	Alto	[AP_SCom]	Sistema de gestión Comercial ERP	Errores de mantenimiento / actualización de software.	Compatibilidad del ERP (sistemas operativos y versión de aplicaciones de ofimática).	9	4	6	Debe ser tratado
R61	Alto	[AP_SCom]	Sistema de gestión Comercial ERP	Indisponibilidad de soporte proveedor.	Ausencia de contractos comerciales y de acuerdos de SLA.	9	6	12	Tolerable
R63	Alto	[AP_SFE]	Sistema de facturación electrónica	Errores de mantenimiento / actualización de software	Carencia de un plan de actualización de software.	9	6	15	Tolerable
R14	Medio	[HW_SrvApli]	Servidor de aplicaciones	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (Generador eléctrico, UPS)	8	4	6	Debe ser tratado
R23	Medio	[HW_SerTerm]	Servidores de terminales remotas	Errores de mantenimiento y actualización de software.	Inadecuado control de mantenimiento y actualización de software.	8	6	10	Tolerable
R24	Medio	[HW_SerTerm]	Servidores de terminales remotas	Agotamiento de recursos de hardware.	Inadecuado dimensionamiento de hardware (disco duro, memoria ram, etc.,)	8	6	8	Tolerable
R26	Medio	[HW_SerVpn]	Servidor de VPN y Firewall	Denegación de servicios.	Carencia de un sistema de información de administración de eventos y monitoreo de red (log).	8	6	8	Tolerable

MATRIZ DE PRIORIZACIÓN Y CONTROL DE RIESGOS									
RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R29	Medio	[HW_SerVpn]	Servidor de VPN y Firewall	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (Generador eléctrico, UPS)	8	4	6	Debe ser tratado
R36	Medio	[HW_EIU]	Equipos de informáticos deusuario	Avería de hardware	Carencia de un plan de seguridad física.	8	6	8	Tolerable
R40	Medio	[HW_EIU]	Equipos de informáticos deusuario	Agua (Inundaciones, fugas)	Deficiencia de infraestructura para instalación de equipos.	8	4	8	Tolerable
R48	Medio	[HW_RedCom]	Equipos de comunicación	Agua (Inundaciones, fugas)	Infraestructura inadecuada para instalación de equipos.	8	5	8	Tolerable
R58	Medio	[AP_SCom]	Sistema de gestión Comercial ERP	Errores de programación y validación.	Carencia de buenas prácticas de programación. (Inyección SQL, validación de entrada de datos.)	8	4	6	Debe ser tratado
R70	Medio	[MED_DExt]	Discos de almacenamiento externo	Avería de tipo lógico	Intrusión de software malicioso en medios de almacenamiento externo.	8	6	10	Tolerable
R73	Medio	[S_GesComl]	Servicio de Gestión Comercial	Indisponibilidad del administrador del sistema	Inadecuado programa de capacitación al personal.	8	8	12	Tolerable
R77	Medio	[S_PWeb]	Servicio página Web corporativa	Indisponibilidad del administrador del sistema	Dependencia excesiva del administrador de la página web	8	6	12	Tolerable
R83	Medio	[S_EMail]	Servicio de Correo Electrónico	Falla del archivo de correo del usuario	Ausencia de políticas de mantenimiento de cliente de correo.	8	6	10	Tolerable
R1	Medio	[ED_CDatos]	Centro de datos.	Pertubación de la red eléctrica.	Inadecuado dimensionamiento y cableado de fluido eléctrico del DataCenter.	6	4	6	Tolerable

MATRIZ DE PRIORIZACIÓN Y CONTROL DE RIESGOS									
RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R11	Medio	[HW_SrvApli]	Servidor de aplicaciones	Error de mantenimiento y actualización de software.	Inadecuado control de mantenimientos y actualización de software.	6	4	9	Tolerable
R32	Medio	[HW_EIU]	Equipos de informáticos de usuario	Avería de software	Inadecuado control de actualización de software.	6	6	12	Tolerable
R35	Medio	[HW_EIU]	Equipos de informáticos de usuario	Avería de hardware	Incumplimiento del plan de mantenimiento de equipos (hardware).	6	6	9	Tolerable
R37	Medio	[HW_EIU]	Equipos de informáticos de usuario	Hurto de equipos	Deficiencia de procedimientos de control de salida e ingresos de equipos.	6	6	9	Tolerable
R45	Medio	[HW_RedCom]	Equipos de comunicación	Avería de equipos de comunicación.	Ausencia de políticas de mantenimiento preventivo de los equipos de comunicación.	6	6	8	Tolerable
R5	Medio	[ED_CDatos]	Centro de datos.	Agua (Inundaciones, fugas)	Cercanía a los ductos de ventilación, techos aligerados y suelo.	6	6	8	Tolerable
R55	Medio	[AP_SCom]	Sistema de gestión Comercial ERP	Errores de mantenimiento / actualización de software.	Carencia de documentación técnica.	6	4	6	Tolerable
R66	Medio	[AP_SVMov]	Sistema de venta móvil	Errores de mantenimiento / actualización de software	Carencia de un plan de actualización de software.	6	4	9	Tolerable
R7	Medio	[ED_CDatos]	Centro de datos.	Errores Humanos de operadores.	Carencia de buenas prácticas de operación y mantenimiento.	6	4	9	Tolerable
R74	Medio	[S_GesCom]l	Servicio de Gestión Comercial	Indisponibilidad del administrador del sistema	Dependencia excesiva del administrador del software.	6	4	6	Tolerable

MATRIZ DE PRIORIZACIÓN Y CONTROL DE RIESGOS									
RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R75	Medio	[S_PWeb]	Servicio página Web corporativa	Error de usuario.	Carencia de validación de datos entradas del usuario.	6	6	9	Tolerable
R76	Medio	[S_PWeb]	Servicio página Web corporativa	Acceso no Autorizado.	Carencia de un sistema de información para administración de eventos.	6	6	9	Tolerable
R85	Medio	[S_EMail]	Servicio de Correo Electrónico	Difusión de software dañino	Ausencia de políticas de seguridad y capacitación al usuario.	6	4	6	Tolerable
R9	Medio	[ED_CDatos]	Centro de datos.	Obsolescencia tecnológica.	Falta de un plan de control de cambios de equipos según la vida útil y/o demanda operacional.	6	4	6	Tolerable
R17	Medio	[HW_SrvBD]	Servidor de base de datos ERP	Error de configuración de hardware.	Carencia de un plan de gestión de cambios.	5	3	5	Tolerable
R4	Medio	[ED_CDatos]	Centro de datos.	Fuego (Incendio)	Carencia de sistema de seguridad, planes y procedimientos contra incendio.	5	2	3	Debe ser tratado
R41	Medio	[HW_EIU]	Equipos de informáticos de usuario	Desastres naturales.	Carencia de pólizas de seguro.	5	6	8	Tolerable
R49	Medio	[HW_RedCom]	Equipos de comunicación	Desastres naturales.	Carencia de pólizas de seguro.	5	5	10	Tolerable
R6	Medio	[ED_CDatos]	Centro de datos.	Desastres naturales.	Carencia de pólizas de seguro.	5	2	3	Debe ser tratado
R18	Medio	[HW_SrvBD]	Servidor de base de datos ERP	Agotamiento de recursos de hardware.	Inadecuado dimensionamiento de hardware (disco duro, memoria ram, etc.,)	4	3	5	Tolerable

MATRIZ DE PRIORIZACIÓN Y CONTROL DE RIESGOS									
RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R20	Medio	[HW_SerTerm]	Servidores de terminales remotas	Denegación de acceso servicio.	Carencia de licenciamiento y soporte del servicio RDP.	4	4	5	Tolerable
R28	Medio	[HW_SerGit]	Servidor de Gitlab	Error de mantenimiento y actualización de software.	Inadecuado control de mantenimientos y actualización de software.	4	4	6	Tolerable
R3	Medio	[ED_CDatos]	Centro de datos.	Falla de equipos de climatización (aire acondicionado).	Inadecuado programa de mantenimiento de equipos del aire acondicionado.	4	4	6	Tolerable
R30	Medio	[HW_EIU]	Equipos de informáticos de usuario	Obsolescencia tecnológica de equipos de cómputo.	Carencia de un plan de cambios de equipos de cómputo de acuerdo a su vida útil.	4	3	4	Tolerable
R39	Medio	[HW_EIU]	Equipos de informáticos de usuario	Fuego (Incendio)	Carencia de sistema de seguridad contra incendio, planes y procedimientos contra incendio.	4	2	4	Tolerable
R47	Medio	[HW_RedCom]	Equipos de comunicación	Fuego (Incendio)	Carencia de sistema de seguridad, planes y procedimientos contra incendio.	4	4	5	Tolerable
R78	Medio	[S_Wifi]	Servicio de Wifi	Uso no previsto	Ausencia de políticas de uso del servicio.	4	8	12	Tolerable
R84	Medio	[S_EMail]	Servicio de Correo Electrónico	El aumento de la necesidades de ancho de banda y almacenamiento	Ausencia de políticas de uso del correo.	4	8	12	Tolerable
R12	Bajo	[HW_SrvApli]	Servidor de aplicaciones	Error de mantenimiento y actualización de software.	Intrusión de software malicioso.	3	3	6	Tolerable

MATRIZ DE PRIORIZACIÓN Y CONTROL DE RIESGOS									
RIESGO		Código Activo	Activo	AMENAZA	VULNERABILIDAD	Magnitud PxI	Apetito	Tolerancia	Nivel de Decisión
Código	Nivel								
R31	Bajo	[HW_EIU]	Equipos de informáticos de usuario	Avería de software	Carencia de licencias de software de sistema operativo.	3	4	6	Tolerable
R53	Bajo	[AP_SBDWeb]	BD Página web	Acceso no autorizado.	Modificación no autorizada de BD y configuraciones.	3	4	6	Tolerable
R54	Bajo	[AP_SBDWeb]	BD Página web	Acceso no autorizado.	Carencia de auditoría detallada de acceso y acciones ejecutadas a la base de datos.	3	4	6	Tolerable
R79	Bajo	[S_Wifi]	Servicio de Wifi	Acceso no Autorizado	Ausencia de controles de acceso a usuarios.	3	3	8	Tolerable

Fase IV: Tratamiento del Riesgo

4.1. Estrategias de Tratamiento

Las estrategias de protección para gestionar los riesgos son mitigar, evitar, trasferir, aceptar.

- Modificar-Mitigar: Ejecutar acciones para prevenir y controlar la probabilidad o frecuencia e impacto de los riesgos.
- Evitar: cuando se decide no emprender o dejar de realizar actividades que da lugar a una acción riesgosa
- Transferir-Compartir: se refiere a asegurar y equilibrar los riesgos, compartiéndolos con terceros que pueda manejar el riesgo en particular de manera más efectiva.
- Retención-Aceptar: aceptar el cierto riesgo de un modo costo-efectivo, es decir se conoce el riesgo y se establece la decisión de conservar el riesgo sin tomar medidas adicionales.

4.2. Preparación e implementación de los planes de tratamiento del riesgo

PLANES DE TRATAMIENTO DEL RIESGO											
Código: PRY01 **Nombre del Proyecto:** Mejoramiento de la red de datos empresarial + Seguridad gestionada			**Fecha de elaboración:** 19.03.209 **Elaborado Por:** Wilson Cruz Cabrera – Jefe de Sistemas				**Revisado Por:** Gerencia General. **Fecha: 22.04.2019**				
RIESGO			**PLAN DE TRATAMIENTO**								
Código	**Cód. Activo**	**Nivel**	**Tratamiento**	**Acciones**	**Puntaje Aceptable**	**Objetivo**	**Responsable**	**Recursos**	**Proceso Afectado**	**Tiempo de ejecución**	**Presupuesto**
R80	[S_Internet]	Muy Alto	Mitigar	Contratar un servicio de internet de fibra óptica con conexión VPN para enlazar todas las sedes. Implementar dispositivos modem 4G como respaldo.	6	Reducir el índice de no disponibilidad del servicio de internet.	- Jefe de Sistemas - Proveedor del servicio.	Jefe de sistemas (Trabajo 30%) -Switch Core -Modem 4G	Ventas Compras Tesorería Contabilidad RRHH Créditos Inventario Almacén	40 días hábiles (total de 96 horas [8*40*30%])	Inversión mensual enlaces de internet. =S/22,400 Modem 4G ilimitado Costo mensual =S/1,350. (S/79 x 17 locales). Nro. Personas*tiempo*costohora =1*96*30 =S/2,880 Adquisición de Switch Core Sisco $/3,500 Total Inversión S/23,750 Mensual
R13	[HW_Srv Apli]	Alto									
R21	[HW_Ser Term]	Alto									
R27	[HW_SerVpn]	Alto									
R81	[S_Internet]	Alto	Mitigar	Contratar el servicio de seguridad gestionada con Fortinet.	3	Reducir el índice de uso no previsto de acceso a internet.					

PLANES DE TRATAMIENTO DEL RIESGO											
Código: PRY02 **Nombre del Proyecto:** Implementar proceso de auditoría de acceso al servidor de base de datos.			**Fecha de elaboración:** 02.04.2019 **Elaborado Por:** Wilson Cruz Cabrera – Jefe de Sistemas					**Revisado Por:** Gerencia General **Fecha: 22.04.2019**			
RIESGO			**PLAN DE TRATAMIENTO**								
Código	**Cód. Activo**	**Nivel**	**Tratamiento**	**Acciones**	**Puntaje Aceptable**	**Objetivo**	**Responsable**	**Recursos**	**Proceso Afectado**	**Tiempo de ejecución**	**Presupuesto**
R50 R51	[AP_SBDErp]	Muy Alto	Mitigar	Establecer un proceso de monitoreo sobre la información de la base de Datos. Contratar un DBA para centralización de la administración de la base de datos. Implementar políticas de acceso a la BD.	4	Obtener reportes de auditorías de manipulación de datos y performance de la BD	Jefe de Sistemas	-Jefe de sistemas (DBA Trabajo al 50%) -Software SQL Diagnostic Manager para auditoria	Ventas Compras Tesorería Contabilidad RRHH Créditos Inventario Almacén	Un Mes (30 días hábiles total 120 horas [4*30])	Nro. Personas* tiempo*costohora 1*120*30 =S/3,600. Adquisición de Software$ 1,996*3.285 =S/6,556 Total de Inversión S/10,157
R15	[HW_SrvBD]	Muy Alto	Mitigar	Implementación de directivas de grupo por GPO.	4	Registrar acciones de accesos de usuarios.	Jefe de Sistemas.	-Jefe de sistemas (Trabajo al 50%)	Ventas Compras Tesorería Contabilidad RRHH Créditos Inventario Almacén	Cinco días hábiles (Total de 20 horas)	Nro. Personas* tiempo*costohora 1*120*30 =S/585

PLANES DE TRATAMIENTO DEL RIESGO											
Código: PRY03 **Nombre del Proyecto:** Mejoramiento de infraestructura y controles de acceso al centro de datos.			**Fecha de elaboración:** 04.03.2019 **Elaborado Por:** Wilson Cruz Cabrera – Jefe de Sistemas					**Revisado Por:** Gerencia General **Fecha: 20.03.2019**			
RIESGO			**PLAN DE TRATAMIENTO**								
Código	**Cód. Activo**	**Nivel**	**Tratamiento**	**Acciones**	**Puntaje Aceptable**	**Objetivo**	**Responsable**	**Recursos**	**Proceso Afectado**	**Tiempo de ejecución**	**Presupuesto**
R8	[ED_CDatos]	Muy Alto	Mitigar	-Registrar los accesos al centro de datos mediante una Bitácora. -Instalar cámara de vigilancia en el centro de datos y lector biométrico. -Implementar políticas de condiciones de acceso al centro de datos.	4	Monitorizar, controlar el acceso al centro de datos.	Jefatura de sistemas. Gerencia de Finanzas	-Jefe de sistemas. (Trabajo al 30% total de 48 horas [8*20*30%]) - Libro de bitácoras. - Cámara de video vigilancia. -Lector de biometría.	Ventas Compras Tesorería Contabilidad RRHH Créditos Inventario Almacén	Veinte días hábiles de instalación	Nro. Personas*tiempo*costohora 1*48*30 S/1,440. Adquisición de Cámaras de video vigilancia S/5,000 Lector biometría y control de puerta. S/3,500 Total Inversión S/9,940

PLANES DE TRATAMIENTO DEL RIESGO											
Código: PRY03 **Nombre del Proyecto:** Mejoramiento de infraestructura y controles de acceso al centro de datos.			**Fecha de elaboración:** 04.03.2019 **Elaborado Por:** Wilson Cruz Cabrera – Jefe de Sistemas					**Revisado Por:** Gerencia General **Fecha: 20.03.2019**			
RIESGO			**PLAN DE TRATAMIENTO**								
Código	**Cód. Activo**	**Nivel**	**Tratamiento**	**Acciones**	**Puntaje Aceptable**	**Objetivo**	**Responsable**	**Recursos**	**Proceso Afectado**	**Tiempo de ejecución**	**Presupuesto**
R2	[ED_CDatos]	Muy Alto	Mitigar	Implementar un sistema de alimentación ininterrumpida. Implementar plan de uso y mantenimiento del sistema de alimentación eléctrica.	6	Asegurar la alimentación de energía de los activos críticos de operación de ventas.	Jefatura de Sistemas Gerencia de finanzas	Generador eléctrico de 12kva. Estabilizador de 8kva UPS de 6Kva (Autonomía mínima de 15 minutos)	Ventas Contabilidad Tesorería Compras	Un mes	Generador eléctrico $2,100*3.328 Estabilizador S/3,500 UPS S/6,500 Instalación S/10,000 Total de inversión S/27,000
R19	[HW_SrvBD]	Alto			4						
R25	[HW_SerTerm]	Alto			4						
R46	[HW_RedCom]	Alto			4						
R14	[HW_SrvApli]	Medio			4						
R29	[HW_SerVpn]	Medio			4						
R4	[ED_CDatos]	Medio	Compartir	-Implementar sistemas de control contra incendios y monitoreo. -Implementar planes de capacitación al personal para eventos de fuego.	2	-Detección temprana de humo y activar la alarma central de emergencias. -Minimizar el número de emergencias contra incendios. -Reducir el impacto frente a eventos de fuego.	Gerente Finanzas Jefatura de Sistema Proveedor servicio monitoreo.	Equipamiento para detención y control de incendio. Jefes de áreas administrativas.	Ventas Inventario Almacén Compras Tesorería	Un mes. Veinte días de implementación. 10 días de capacitación al personal.	Costo de seguro contra incendio S/1,500 (S/90 x 17 locales) Capacitación. S/2,550 (S/150*17 locales)

PLANES DE TRATAMIENTO DEL RIESGO											
Código: PRY03 **Nombre del Proyecto:** Mejoramiento de infraestructura y controles de acceso al centro de datos.			**Fecha de elaboración:** 04.03.2019 **Elaborado Por:** Wilson Cruz Cabrera – Jefe de Sistemas					**Revisado Por:** Gerencia General **Fecha: 20.03.2019**			
RIESGO			**PLAN DE TRATAMIENTO**								
Código	**Cód. Activo**	**Nivel**	**Tratamiento**	**Acciones**	**Puntaje Aceptable**	**Objetivo**	**Responsable**	**Recursos**	**Proceso Afectado**	**Tiempo de ejecución**	**Presupuesto**
R6	[ED_CDatos]	Medio	Compartir	Contratar seguro para riesgos patrimoniales. Implementar planes de capacitación al personal para eventos de desastres naturales.	2	Minimizar el número de emergencias contra desastres naturales. Reducir el impacto frente a desastres naturales.	Gerencia de finanzas Jefatura de sistemas. Proveedor de seguro.	. Consejería legal.	Ventas Compras Tesorería Contabilidad RRHH Créditos Inventario	5 días hábiles	Costo de seguro S/2,700 Mensual. Costo de Capacitación. S/255 (S/50*17 locales)

PLANES DE TRATAMIENTO DEL RIESGO											
Código: PRY04 **Nombre del Proyecto:** Definir e implementar políticas de copias de seguridad automatizada.			**Fecha de elaboración:** 06.05.2019					**Revisado Por:** Directorio de la Gerencia General			
			Elaborado Por: Wilson Cruz Cabrera – Jefe de Sistemas					**Fecha: 20.05.2019**			
RIESGO			**PLAN DE TRATAMIENTO**								
Código	**Cód. Activo**	**Nivel**	**Tratamiento**	**Acciones**	**Puntaje Aceptable**	**Objetivo**	**Responsable**	**Recursos**	**Proceso Afectado**	**Tiempo de ejecución**	**Presupuesto**
R69	[MED_DExt]	Muy Alto	Mitigar	Desarrollar e implementar políticas de copia de seguridad y restauración de información crítica.	4	Asegurar la continuidad del negocio, proceso o actividad.	Gerencia General, (Aprobación) Área de sistemas. (Trabajo al 50%)	Jefe de sistemas. (Trabajo 50%) Software Bacula para copia de seguridad automatizada. Dispositivos de soporte para copias de seguridad.	Ventas Compras Tesorería Contabilidad RRHH Créditos Inventario	Un mes (Total de 120 horas [8*30*50%]).	Desarrollo de la política =1*120hr *30costohora =S/3,600 Dispositivos de almacenamiento externo. S/230 c/u Solución Cloud. S/0.80 por GB mensual Capacitación. S/850 (S/30hr *17 locales)
R34	[HW_EIU]				6						

PLANES DE TRATAMIENTO DEL RIESGO												
Código: PRY05 **Nombre del Proyecto:** Evaluación e implementación de un nuevo ERP empresarial.			**Fecha de elaboración:** 20.05.2019								**Revisado Por:** Directorio de la Gerencia General	
			Elaborado Por: Wilson Cruz Cabrera – Jefe de Sistemas								**Fecha: 03.06.2019**	
RIESGO			**PLAN DE TRATAMIENTO**									
Código	**Cód. Activo**	**Nivel**	**Tratamiento**	**Acciones**	**Puntaje Aceptable**	**Objetivo**	**Responsable**	**Recursos**	**Proceso Afectado**	**Tiempo de ejecución**	**Presupuesto**
R59	[AP_SCom]	Alto	Mitigar	Implementación presupuestaria. Implementación del software (incluye capacitación).	4	Automatizar todos los procesos de negocio. Eliminación de datos y operaciones innecesarias. -Mejor toma de decisiones.	Directorio de la empresa. Jefatura de Sistemas Propietarios del proceso (Jefes administrativos y operación comercial). Proveedor de Software ERP	-Gerencia General -Gerencia Adjunta -Gerencia Finanzas -Gerencia comercial -Personal clave (Key user 10) - Adquisición de infraestructura de servidores. -Equipo de del proveedor.	Ventas Compras Importaciones Tesorería Contabilidad RRHH Créditos Inventario Distribución	8 Meses de implantación Uso de personal interno 256 horas (2 sesiones por semana media Jornada). Fórmula [8hr semanal * 4 semanas *8meses]	Costo de la solución ERP $369,723 Nro. Personas* tiempo*costohora 14*256*20 =S/71,000
R62		Alto			3						
R57		Alto			4						
R58		Medio			4						

Fase V: Comunicación y consulta

PLAN DE GESTIÓN DE COMUNICACIÓN Y CONSULTA							
Proceso de comunicación	**Descripción de Actividad**	**Emisor**	**Receptor(es)**	**Resultado de la comunicación (Información)**	**Aprobado por**	**Periodo de vigencia**	**Canal de comunicación**
Entradas	Gestionar las expectativas de los interesados.	Gerencia de finanzas	Jefatura de sistemas	Plan estratégico organizacional.	Gerencia General	Una sola vez.	Primera reunión.
	Definir alcance y criterios a considerar para evaluar los riesgos.	Gerencia general adjunta.	-Gerente de finanzas -Jefatura de sistemas	Registro de requerimientos de operación.	Gerencia General	A demanda.	Reuniones de trabajo.
Proceso: Herramientas y técnicas.	Priorizar los procesos de negocio.	Jefes de áreas administrativas. (Dueños de procesos)	-Jefatura de sistemas -Gerente de finanzas	Cuadro de análisis BIA	Gerencia General	A demanda.	Reuniones de trabajo. Correo electrónica.
	Evaluar las amenazas identificadas.	Jefatura de sistemas	-Jefes de áreas administrativas. (Dueños de procesos) -Gerente de finanzas -Gerencia general adjunta.	Cuadro de análisis de riesgos.	Gerencia General	A demanda.	Reuniones de trabajo. Correo electrónico.
	Priorizar los riesgos y acciones de tratamiento.	Jefatura de Sistemas	-Jefes de áreas administrativas. (Dueños de procesos) -Gerente de finanzas -Gerencia general adjunta.	Matriz de priorización y control de Riesgos	Gerencia General	A demanda.	Reuniones de trabajo. Correo electrónico.

PLAN DE GESTIÓN DE COMUNICACIÓN Y CONSULTA							
Proceso de comunicación	**Descripción de Actividad**	**Emisor**	**Receptor(es)**	**Resultado de la comunicación (Información)**	**Aprobado por**	**Periodo de vigencia**	**Canal de comunicación**
Salidas.	Proyectos y acciones de salvaguardas.	Jefatura de sistemas.	-Jefes de áreas administrativas. (Dueños de procesos) -Gerente de finanzas -Gerencia general adjunta.	Planes de tratamiento del riesgo.	Gerencia General	A demanda.	Reuniones de trabajo. Correo electrónico.
	Construir un sentido de inclusión a las personas afectadas por el riesgo.	Jefatura de sistemas.	- Jefes de ventas -Jefes de áreas administrativas. (Dueños de procesos) -Gerente de finanzas -Gerencia general adjunta.	Planes de capacitación.	Gerencia General	A demanda.	Reuniones de trabajo. Correo electrónico.

Fase VI: Seguimiento y Revisión

SEGUIMIENTO Y REVISIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS		
RIESGO	**Código:**	**PRY01**
	Nombre del Proyecto:	Mejoramiento de la red de datos empresarial + Seguridad gestionada
	Riesgo que se trata:	R80: Muy Alto, R13: Alto, R21: Alto, R27: Alto R81: Alto
	Nivel máximo de criticidad de los activos que se trata:	Muy Alto
PLAN DE TRATAMIENTO	**Estrategía de riesgo:**	Mitigar
	Acciones a realizar:	-Contratar un servicio de internet de fibra óptica con conexión VPN para enlazar todas las sedes. - Implementar dispositivos modem 4G como respaldo. - Contratar el servicio de seguridad gestionada con Fortinet.
	Puntaje aceptable	R80(6), R13(6), R21(6), R27(6),R81(3)
	Objetivo:	- Reducir el índice de no disponibilidad del servicio de internet.
	Responsable:	- Jefatura de Sistemas.
	Recursos:	-Jefe de Sistemas (Trabajo 30%) -Switch Core -Modem 4G
	Proceso Afectado (Identificador/Nombre)	Ventas, Compras, Tesorería, Contabilidad RRHH, Créditos, Inventario, Almacén.
	Tiempo de ejecución	40 días hábiles
	Presupuesto	Total Inversión: S/2,880+($3,500*3.285)=S/14,337 Costo recurrente mensual: S/22,400+1,350=S/23,750
SEGUIMIENTO Y REVISIÓN	**Verificación de Resultados:**	**Indicadores**
	Registro de incidencias por fallos de conexión de internet. Cumplimientos de los SLA del proveedor.	Número de veces de no disponibilidad del servicio de internet. Tiempo transcurrido de no disponibilidad del servicio de internet. Nivel de satisfación del usuario.
	Análisis de Resultados	
	- Se ha mejorado la disponibilidad del servicio de red interna de Chiclayo e internet en 50%,	
	Acciones para mejorar el proyecto (Retroalimentación)	
	- Concluir la implementación del proyecto con conexión VPN para enlazar todas las sedes a fin de mantener alta disponibilidad integrando la red WAN, solo se ha implementado en la cabecera Switch core, internet de respaldo y equipo de seguridad Fortinet.	

SEGUIMIENTO Y REVISIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS		
RIESGO	**Código:**	**PRY03**
	Nombre del Proyecto:	Mejoramiento de infraestructura y controles de acceso al centro de datos.
	Riesgo que se trata:	R8: Muy Alto,R2:Muy Alto,R19:Alto,R25:Alto,R46:Alto, R14:Medio,R29:Medio,R4:Medio,R6:Medio
	Nivel máximo de criticidad de los activos que se trata:	Muy Alto
PLAN DE TRATAMIENTO	**Estrategía de riesgo:**	Mitigar y Compartir
	Acciones a realizar:	-Registrar los accesos al centro de datos mediante una Bitácora. -Instalar cámara de vigilancia en el centro de datos y lector biométrico. -Implementar políticas de condiciones de acceso al centro de datos. -Implementar un sistema de alimentación ininterrumpida. -Implementar plan de uso y mantenimiento del sistema de alimentación eléctrica. -Implementar sistemas de control contra incendios y monitoreo. -Implementar planes de capacitación al personal para eventos de fuego y desastres naturales. -Contratar seguro para riesgos patrimoniales.
	Puntaje acceptable:	R8(3),R2(6),R19(4),R25(4),R46(4),R14(4),R29(4),R4(2),R6(2)
	Objetivo:	-Monitorizar, controlar el acceso al centro de datos. - Asegurar la alimentación de energía de los activos críticos de operación de ventas. -Detección temprana de humo y activar la alarma central de emergencias contra incendios. -Minimizar el número de emergencias contra incendios. -Reducir el impacto frente a eventos de fuego.
	Responsable:	Jefatura de Sistemas Gerencia de Finanzas
	Recursos:	-Generador eléctrico de 12kva. -Estabilizador de 8kva -UPS de 6Kva (Autonomía mínima de 15 minutos) -Equipamiento para detención y control de incendio. -Jefes de áreas administrativas. -Consejería legal.
	Proceso Afectado (Identificador/Nombre)	Ventas, Compras, Tesorería, Contabilidad, RRHH, Créditos, Inventario.
	Tiempo de ejecución	Un mes.
	Presupuesto	Costo Inversión: 9,940+27,000+2,550+255=S/39,745 Costos recurrentes mensual: 1500+2,700=S/4,200

SEGUIMIENTO Y REVISIÓN		
	Verificación de Resultados:	**Indicadores**
	-Registro de incidencias por corte de energía eléctrica. -Registro de incidencias eventos por evento de fuego. -Registro de incidencias por desastres naturales.	R8: Cantidad de accesos no autorizados. R2, R19, R25, R46, R14, R29: Tiempo de inactividad de las operaciones por corte de energía eléctrica. R4: Porcentaje de pérdida económica por evento de fuego. R6: Porcentaje de pérdida económica por evento de desastres naturales.
	Análisis de Resultados	
	- Se redujo el Tiempo de inactividad de las operaciones por corte de energía eléctrica de 4 horas promedio a 20 minutos para conexión a los servicios del centro de datos. - Número de acceso no autorizado (se está en proceso de medición por implementarse recientemente)	
	Acciones para mejorar el proyecto (Retroalimentación)	
	- Se debe revisar si los seguros propuestos son suficientes para proteger el valor de los equipos informáticos. - Actualizar constantemente el inventario de activos informáticos para su registro patrimonial en la empresa.	

Fase VII: Registro e informe

REGISTRO E INFORME											
Código:	**PRY01**										
Nombre del Proyecto:	Mejoramiento de la red de datos empresarial + Seguridad gestionada										
Preparado por:	Ing. Wilson Cruz Cabrera										
Fecha:	03.06.2019										
Lección Aprendida Nro.: ***LA-1***											
Lección Aprendida: *Revisión de las Contrataciones y Adquisiciones*											
Rol en el Equipo del Proyecto: *Jefatura de sistemas*											
Fase del Proceso: *		Identificación de Procesos		Evaluación del Riesgo		Valoración del Riesgo		Tratamiento	X	Seguimiento y Revisión	
Proceso o actividad de Negocio Afectado: Ventas, Compras, Tesorería, Contabilidad, RRHH, Créditos, Inventario.											
¿Resultados de actividades ejecutadas de la gestión del riesgo? *-Se ha mejorado la disponibilidad del servicio de red interna de Chiclayo e internet en 50%.*											
¿Cuál es la lección específica aprendida? *-La implementación debe ser integral a nivel de todas las sedes con el fin de que la disponibilidad de la operación comercial sea completa.* *-Los equipos informáticos que se vienen renovando deben tener tarjetas inalámbricas para conexión Wifi.* *-Los equipos móviles de conexión 4G deben tener puerto de red con conexión RJ45 para conexión directa a un Switch de comunicación.*											
¿Qué acción se tomó y por qué? *Enunciar solo si la opción de tratamiento seleccionada es Aceptar el riesgo.*											
¿Qué comportamiento se recomienda para el futuro? - *Invertir en la solución integral propuesta evaluando el costo beneficio por la no disponibilidad de los servicios de TI.*											
¿Quién debe ser informado sobre esta lección aprendida?: (marcar una)											
	x	Sponsor		Gerente(s) Proyecto	x	Equipo del Proyecto		Todo el Personal			
		Otros:									
¿Cómo debe ser distribuida esta lección aprendida? (marcar todas las que apliquen)											
	x	e-mail		Intranet/pagina Web		Preguntas Frecuentes		Biblioteca			
		Otros:									
¿Ha anexado referencia(s), ejemplo(s) y/o material(es) adicional(es)?			X	si		no					
Nombre(s) de anexo(s): 1. *Propuesta técnica económica de la solución integral de mejoramiento de la red de datos a nivel nacional (OTE: Proveedor de comunicaciones).*											

REGISTRO E INFORME																					
Código:	**PRY03**																				
Nombre del Proyecto:	Mejoramiento de infraestructura y controles de acceso al centro de datos.																				
Preparado por:	Ing. Wilson Cruz Cabrera																				
Fecha:	03.06.2019																				
Lección Aprendida Nro.: *LA-2*																					
Lección Aprendida: *Control de Infraestructura del Centro de Datos*																					
Rol en el Equipo del Proyecto: *Jefatura de sistemas.*																					
Fase del Proceso: *			Identificación de		Evaluación del		Valoración del		Tratamiento	X	Seguimiento y										
Proceso o actividad de Negocio Afectado: Ventas, Compras, Tesorería, Contabilidad, RRHH, Créditos, Inventario.																					
¿Resultados de actividades ejecutadas de la gestión del riesgo? *-Se redujo el Tiempo de inactividad de las operaciones por corte de energía eléctrica de 4 horas promedio a 20 minutos para conexión a los servicios del centro de datos.*																					
¿Cuál es la lección específica aprendida? *-La implementación del sistema de alimentación ininterrumpida debe ser integral incluyendo UPS para que el servicio permanezca activo mientras se enciende el generador eléctrico y apertura las cuchillas de transferencia de entrada de energía.*																					
¿Qué acción se tomó y por qué? *Enunciar solo si la opción de tratamiento seleccionada es Aceptar el riesgo.*																					
¿Qué comportamiento se recomienda para el futuro? *-Invertir en la solución integral propuesta evaluando el costo beneficio por la no disponibilidad de los servicios de TI.* *-Implementar soluciones Hosting o Housing.*																					
¿Quién debe ser informado sobre esta lección aprendida?: (marcar una)																					
	x	Sponsor		Gerente(s) Proyecto		x	Equipo del Proyecto		Todo el Personal												
		Otros:																			
¿Cómo debe ser distribuida esta lección aprendida? (marcar todas las que apliquen)																					
	x	e-mail		Intranet/pagina Web			Preguntas Frecuentes		Biblioteca												
		Otros:																			
¿Ha anexado referencia(s), ejemplo(s) y/o material(es) adicional(es)?										**X**	**si**		**no**								
Nombre(s) de anexo(s): 1. *Propuesta técnica económica de la solución integral para mejoramiento de infraestructura y controles de acceso al centro de datos.*																					

Anexo 5: Análisis conceptual de estándares y metodologías de gestión del riesgo

Norma / Metodología	ISO 31000: 2018	ISO 27005: 2018	MARGERIT	OCTAVE
Conceptos	✓ Estándar internacional que proporciona directrices para gestionar el riesgo al que se enfrentan las Organizaciones.	✓ Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información.	✓ Metodología de análisis y gestión de riesgos de TI desarrollado por el gobierno español.	✓ Metodología de gestión del riesgo, define una evaluación estratégica basada en riesgos y la planificación técnica de la seguridad.
Principales Características	✓ Asistir a la organización en integrar la gestión del riesgo en todas sus actividades y funciones significativas. ✓ Gobernanza y liderazgo. ✓ Creación y protección del valor. ✓ Supervisión sistémica. ✓ Contexto organizacional. ✓ Comunicación y consulta.	✓ La norma suministra las directrices para la gestión de riesgos de seguridad de la información. ✓ Diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información.	✓ La Metodología describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo, contempla aspectos prácticos para la realización.	✓ Construcciones de los perfiles de amenazas basados en activos. ✓ Identificación de la infraestructura de vulnerabilidad. ✓ Desarrollo de planes y estrategias de seguridad.
Fases	1. Comunicación y consulta 2. Alcance, contexto y criterios. 3. Evaluación del riesgo a) Identificación del riesgo. b) Análisis del riesgo. c) Valoración del riesgo.	1. Establecer el contexto 2. Evaluación del Riesgo a) Identificación del riesgo. b) Análisis del riesgo. c) Evaluación del riesgo. • Decisión sobre el riesgo. Evaluación satisfactoria.	1. Análisis de riesgos. 2. Caracterización de los activos: a. Caracterización de las amenazas b. Caracterización de las salvaguardas c. Estimación del estado del riesgo.	1.Visión de organización. a. Activos b. Amenazas c. Prácticas actuales d. Vulnerabilidades de la organización e. Cumplimiento

Norma / Metodología	ISO 31000: 2018	ISO 27005: 2018	MARGERIT	OCTAVE
Fases	4. Tratamiento del Riesgo 5. Seguimiento y revisión 6. Registro e informe	3. Tratamiento del riesgo • Decisión sobre el riesgo. Tratamiento satisfactorio 4. Aceptación del riesgo 5. Monitoreo y revisión del riesgo 6. Comunicación del riesgo y consulta.	3. Gestionar los riesgos	2. Visión Tecnológica. a. Vulnerabilidades tecnológicas 3. Planificación de las medidas y reducción de riesgos a. Riesgos b. Estrategias de protección c. Planes de atenuación
Ámbito de aplicación	✓ La aplicación de sus directrices puede adaptarse a cualquier organización y a su contexto.	✓ ISO-27005 es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos de seguridad de la información.	✓ Análisis y gestión de riesgos de los sistemas de información: Gobierno, Organismos, compañías grandes, PYME, compañías comerciales y no comerciales.	✓ Análisis de riesgos para seguridad de sistemas de información: PYMES
Ventajas	✓ Proporciona un enfoque común para gestionar cualquier tipo de riesgo. ✓ Impulsa la necesidad de identificación y tratamiento del riesgo.	✓ Ayuda a crear los SGSI eficaz. ✓ Aborda los riesgos de manera eficaz y oportuna, donde y cuando sea necesario.	✓ Es metódica y detallada por lo que se hace fácil su comprensión. ✓ Posee un extenso archivo de inventarios en lo referente a Recursos de TI, Amenazas y tipo de Activos.	✓ Involucra a todo el personal de la organización. ✓ Se considera de las más completas, ya que involucra como elementos de su modelo de análisis: procesos, activos y dependencias, recursos, vulnerabilidades, amenazas y salvaguardas.

Norma / Metodología	ISO 31000: 2018	ISO 27005: 2018	MARGERIT	OCTAVE
Ventajas	✓ Permite gestionar los riesgos y las oportunidades de modo que aumenta la probabilidad de alcanzar los objetivos. ✓ Asegura la disponibilidad de recursos, económicos financieros y de otro tipo.	✓ Posee la fase de aceptación de riesgos que permite su registro formal del desarrollo a la organización. ✓ Integra todas las actividades de gestión de seguridad de la información tanto para su aplicación como para su operación continua de un SGSI.	✓ Permite un análisis completo cualitativo y cuantitativo. ✓ Soporta herramientas comerciales EAR y NO comerciales PILAR para analizar y valorar los riesgos.	✓ Usa como herramientas de apoyo o aplicación a OCTAVE Automated Tool
Desventajas	✓ No recomienda una metodología para su aplicabilidad en las organizaciones. ✓ No detalla la forma de valorar las amenazas. ✓ No es certificable ✓ No posee herramientas, técnicas, ni comparativas de ayuda para su implementación.	✓ No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial donde se aplica. ✓ No detalla la forma de valorar las amenazas. ✓ No es certificable ✓ No posee herramientas, técnicas, ni comparativas de ayuda para su implementación	✓ No toma en cuenta un análisis de vulnerabilidades. ✓ No toma en cuenta un análisis BIA.	✓ Es aplicable solo a Pymes (pequeña y mediana empresa) ✓ No tiene compatibilidad con estándares. ✓ Presenta varios documentos anexos para llevar a cabo el proceso de análisis de riesgos, lo que la hace tediosa, complicada de entender.

Anexo 6: Armonización de estándares, metodologías y planteamiento del modelo propuesto para la gestión de riesgos

Criterios de Evaluación	Modelo Propuesto	ISO 3100: 2018	ISO 27005: 2018	MARGERIT 3.0	OCTAVE	COBIT RISK IT	ISO 22317:2015
Gobierno del Riesgo de TI en toda la áreas de la organización	1. Alcance, establecer el contexto y criterios.	2. Alcance, Contexto y criterios.	1. Establecimiento del contexto.	Proceso 1: Método.	1. Visión de organización.	1.Actividades de TI.	
Identificar los procesos y actividades críticas del negocio para establecer periodos de tiempo (RTO) y objetivos de operación.	2. Análisis BIA. a. Priorización de procesos y actividades c. Análisis y consolidación.						Procesos del análisis BIA: 1.Planificación y gestión del proyecto. 2. Priorización de productos y servicios. 3. Priorización de procesos. 4. Priorización de actividades. 5. Análisis y consolidación. 6. Obtención de la aprobación de la alta gerencia. 7. Después del BIA – Selección de estrategias de continuidad del negocio.
Gestión de riesgos con enfoque en la protección de activos de TI.	3. Fase de Evaluación del Riesgo. 3.1. Identificación de Activos. a. Tipos y clasificación de activos b. Dependencia de los activos. c. Valoración de los activos.			Proceso 2: Análisis de Riesgo. • Caracterización de los activos. • Caracterización de las amenazas. • Caracterización de las salvaguardas.	Activos • Amenazas • Prácticas actuales. • Vulnerabilidades organizativas • Requerimientos de seguridad.	3. Administración del Riesgo. 2. Evaluar riesgos y oportunidades.	

Criterios de Evaluación	Modelo Propuesto	ISO 3100: 2018	ISO 27005: 2018	MARGERIT 3.0	OCTAVE	COBIT RISK IT	ISO 22317:2015
Considera un alcance completo, para en el análisis como en la gestión de riesgos	3.2. Proceso análisis de riesgos. a. Identificar el riesgo. b. Determinar probabilidad e impacto. 3.3. Proceso valoración de riesgos. a. Valoración del riesgo. b. Priorizar el riesgo 4. Fase tratamiento de riesgos. 4.1. Estrategias de tratamiento. 4.2. Preparación e implementación de planes de tratamiento al Riesgo.	3. Fase de Evaluación del Riesgo. a. Proceso identificación de riesgos. b. Proceso análisis de riesgos. c. Proceso evaluación de riesgos. 4. Fase tratamiento de riesgos.	Proceso 2: Valoración del riesgo Proceso 3: Tratamiento del riesgo Proceso 4: Aceptación del riesgo	• Estimación del estado del riesgo Proceso 3: Gestión del Riesgo • Toma de decisiones • Plan de seguridad • Ejecución del plan	2. Visión Tecnológica Componentes claves. • Vulnerabilidades técnicas. 3. Planificación de las medidas y reducción de riesgos. • Riesgos. • Estrategia de protección. • Planes de mitigación.		
Posee herramientas para inventario de activos y valoración de riesgos.							
Adaptable a cualquier organización y su contexto como empresas comerciales en crecimiento.	5. Fase de Comunicación y consulta. 6. Fase Seguimiento y Revisión. 7. Fase de Registro e informe.	1. Fase de Comunicación y consulta. 5. Fase Seguimiento y Revisión. 6. Fase de Registro e informe.	Proceso 5: Comunicación de los riesgos. Proceso 6: Monitoreo y revisión del riesgo.				
Estándar o metodología que proporciona un lenguaje común a nivel mundial para la gestión de riesgos.							

Anexo 7: Formato de evaluación del modelo (juicio experto)

MATRIZ DE CONSISTENCIA PARA JUICIO EXPERTO

Datos Generales del Experto

Nombres y Apellidos: _____
Grado Académico:_____
Formación académica:_____
Área de experiencia profesional:_____
Tiempo de experiencia:_____
Cargo Actual:_____
Institución donde labora:_____

Objetivo de la investigación: Proponer un modelo de gestión de riesgos de tecnologías de información basados en estándares adaptados en el sector de distribuidoras de la región Lambayeque para contribuir en la protección del activo de TI.

Objetivo de Juicio de Experto: Someter a consulta y validez el modelo de gestión de riesgos de TI aplicadas a empresas distribuidoras de artículos de ferretería, acabados y materiales de construcción de la región Lambayeque.

Escala de calificación: 1: Totalmente en desacuerdo 2: En desacuerdo 3: Ni de acuerdo ni en desacuerdo 4: De acuerdo 5: Totalmente de acuerdo. **Señale con X la opción elegida**

Sub Fase	Objetivo	ESCALA DE LIKERT					Observaciones
		1	2	3	4	5	
FASE I: ALCANCE, CONTEXTO Y CRITERIOS							
Alcance	Definir el alcance de las actividades de gestión del riesgo (estratégico, operacional, de programa, de proyecto)						
Contexto Internos	Comprensión del entorno interno de la organización.						
Contexto Externos	Comprensión del entorno externo en la organización.						
Criterio	Definición de los riesgos empresariales y su importancia como soporte para la toma de decisiones.						
FASE II: ANÁLISIS BIA							
Priorización de procesos y actividades	Definir los procesos y actividades críticas e importantes para continuidad y estabilidad de la organización.						
Análisis y consolidación	Realizar la consolidación de análisis del proceso BIA y los requisitos del negocio para su continuidad de operaciones.						

MATRIZ DE CONSISTENCIA PARA JUICIO EXPERTO							
FASE III: EVALUACIÓN DEL RIESGO							
Identificación de activos	Identificar, clasificar y valorar los activos de TI, que dan soporte a la operatividad de la organización.						
Análisis del riesgo	Identificar las debilidades en la protección del activo (amenazas, vulnerabilidades, probabilidad e impacto).						
Valoración del riesgo	Valorar el riesgo respecto a los resultados obtenidos para su priorización y facilitar la toma de decisiones en la organización.						
FASE IV: TRATAMIENTO DEL RIESGO							
Estrategias de Tratamiento	Determinar la estrategia de tratamiento más apropiado para el rubro de la organización.						
Preparación e implementación de los planes de tratamiento del riesgo	Formular los planes de tratamiento del riesgo y especificar la manera en la que se implementarán las opciones elegidas para el tratamiento.						
FASE V: COMUNICACIÓN Y CONSULTA							
Comunicación y Consulta	Asistir a las partes interesadas a comprender el riesgo y obtener retroalimentación e información para apoyar la toma de decisiones.						
FASE VI: SEGUIMIENTO Y REVISIÓN							
Seguimiento y Revisión	Evaluar periódicamente la eficacia de la gestión del riesgo, registrar resultados, los cambios y proporcionar retroalimentación.						
FASE VII: REGISTRO E INFORME							
Registro e informe	Documentar e informar las decisiones de tratamiento, los resultados y las lecciones aprendidas.						

Anexo 8: Resultado de evaluación de juicio experto

MATRIZ DE CONSISTENCIA PARA JUICIO EXPERTO

Datos Generales del Experto
Nombres y Apellidos: GILBERTO CARRIÓN BARCO
Grado Académico: DOCTOR EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS
Formación académica: INGENIERO EN COMPUTACIÓN E INFORMÁTICA
Área de experiencia profesional: INFRAESTRUCTURA TECNOLOGICA, SEGURIDAD INFORMÁTICA
Tiempo de experiencia: 15 AÑOS
Cargo Actual: CATEDRÁTICO
Institución donde labora: UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Objetivo de la investigación: Proponer un modelo de gestión de riesgos de tecnologías de información basados en estándares adaptados en el sector de distribuidoras de la región Lambayeque para contribuir en la protección del activo de TI.

Objetivo de Juicio de Experto: Someter a consulta y validez el modelo de gestión de riesgos de TI aplicadas a empresas distribuidoras de artículos de ferretería, acabados y materiales de construcción de la región Lambayeque.

Escala de calificación: 1: Totalmente en desacuerdo 2: En desacuerdo 3: Ni de acuerdo ni en desacuerdo 4: De acuerdo 5: Totalmente de acuerdo. **Señale con X la opción elegida**

Sub Fase	Objetivo	ESCALA DE LIKERT					Observaciones
		1	2	3	4	5	
FASE I: ALCANCE, CONTEXTO Y CRITERIOS							
Alcance	Definir el alcance de las actividades de gestión del riesgo (estratégico, operacional, de programa, de proyecto)				X		
Contexto Internos	Comprensión del entorno interno de la organización.				X		
Contexto Externos	Comprensión del entorno externo en la organización.				X		
Criterio	Definición de los riesgos empresariales y su importancia como soporte para la toma de decisiones.				X		
FASE II: ANÁLISIS BIA							
Priorización de procesos y actividades	Definir los procesos y actividades críticas e importantes para continuidad y estabilidad de la organización.				X		
Análisis y consolidación	Realizar la consolidación de análisis del proceso BIA y los requisitos del negocio para su continuidad de operaciones.					X	
FASE III: EVALUACIÓN DEL RIESGO							

Identificación de activos	Identificar, clasificar y valoran los activos de TI, que dan soporte a la operatividad de la organización.					X	
Análisis del riesgo	Identificar las debilidades en la protección del activo (amenazas, vulnerabilidades, probabilidad e impacto).					X	
Valoración del riesgo	Valorar el riesgo respecto a los resultados obtenidos para su priorización y facilitar la toma de decisiones en la organización.					X	
FASE IV: TRATAMIENTO DEL RIESGO							
Estrategias de Tratamiento	Determinar la estrategia de tratamiento más apropiado para el rubro de la organización.				X		
Preparación e implementación de los planes de tratamiento del riesgo	Formular los planes de tratamiento del riesgo y especificar la manera en la que se implementarán las opciones elegidas para el tratamiento.					X	
FASE V: COMUNICACIÓN Y CONSULTA							
Comunicación y Consulta	Asistir a las partes interesadas a comprender el riesgo y obtener retroalimentación e información para apoyar la toma de decisiones.					X	
FASE VI: SEGUIMIENTO Y REVISIÓN							
Seguimiento y Revisión	Evaluar periódicamente la eficacia de la gestión del riesgo, registrar resultados, los cambios y proporcionar retroalimentación.					X	
FASE VII: REGISTRO E INFORME							
Registro e informe	Documentar e informar las decisiones de tratamiento, los resultados y las lecciones aprendidas.					X	

FIRMA DEL EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO EXPERTO

Datos Generales del Experto

Nombres y Apellidos: ERNESTO KARLO CELI ARÉVALO

Grado Académico: DOCTOR EN ADMINISTRACIÓN, MAESTRO EN CIENCIAS CON MENCIÓN EN INFORMÁTICA Y SISTEMAS

Formación académica: INGENIERO DE COMPUTACIÓN Y SISTEMAS

Área de experiencia profesional: SEGURIDAD, CONTROL, AUDITORÍA Y GESTIÓN DE RIESGOS DE TI

Tiempo de experiencia: 25 AÑOS

Cargo Actual: DIRECTOR DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Institución donde labora: UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Objetivo de la investigación: Proponer un modelo de gestión de riesgos de tecnologías de información basados en estándares adaptados en el sector de distribuidoras de la región Lambayeque para contribuir en la protección del activo de TI.

Objetivo de Juicio de Experto: Someter a consulta y validez el modelo de gestión de riesgos de TI aplicadas a empresas distribuidoras de artículos de ferretería, acabados y materiales de construcción de la región Lambayeque.

Escala de calificación: 1: Totalmente en desacuerdo 2: En desacuerdo 3: Ni de acuerdo ni en desacuerdo 4: De acuerdo 5: Totalmente de acuerdo. **Señale con X la opción elegida**

FASE I: ALCANCE, CONTEXTO Y CRITERIOS							
Sub Fase	**Objetivo**	**ESCALA DE LIKERT**					**Observaciones**
		1	2	3	4	5	
Alcance	Definir el alcance de las actividades de gestión del riesgo (estratégico, operacional, de programa, de proyecto)				X		
Contexto Internos	Comprensión del entorno interno de la organización.				X		
Contexto Externos	Comprensión del entorno externo en la organización.				X		
Criterio	Definición de los riesgos empresariales y su importancia como soporte para la toma de decisiones.					X	
FASE II: ANÁLISIS BIA							
Priorización de procesos y actividades	Definir los procesos y actividades críticas e importantes para continuidad y estabilidad de la organización.					X	
Análisis y	Realizar la					X	

consolidación	consolidación de análisis del proceso BIA y los requisitos del negocio para su continuidad de operaciones.						
FASE III: EVALUACIÓN DEL RIESGO							
Identificación de activos	Identificar, clasificar y valorar los activos de TI, que dan soporte a la operatividad de la organización.				X		- La identificación de las dependencias entre activos no se está tomando en cuenta en el cálculo del nivel de exposición al riesgo. Por tanto, es simplemente descriptivo. Magerit tiene técnicas para realizar los cálculos
Análisis del riesgo	Identificar las debilidades en la protección del activo (amenazas, vulnerabilidades, probabilidad e impacto).				X		- Los criterios descritos en las tablas de valoración de activos, probabilidad e impactos se puede mejorar asociándolo con cada uno de los criterios identificados en el ítem 3: operacional, legal, económico y reputacional
Valoración del riesgo	Valorar el riesgo respecto a los resultados obtenidos para su priorización y facilitar la toma de decisiones en la organización.					X	- Sugiero precisar, cuál ha sido el criterio para establecer los niveles de riesgo en el ítem 3-3, porque la distribución de valores no es igual para todos los niveles. No estoy diciendo que está mal, se puede dar estos casos, pero es recomendable precisar cómo se hizo esa distribución. Si no se precisa, se observa como un sesgo
FASE IV: TRATAMIENTO DEL RIESGO							
Estrategias de Tratamiento	Determinar la estrategia de tratamiento más apropiado para el rubro de la organización.					X	
Preparación e implementación de los planes de tratamiento del riesgo	Formular los planes de tratamiento del riesgo y especificar la manera en la que se implementarán las opciones elegidas para el tratamiento.					X	
FASE V: COMUNICACIÓN Y CONSULTA							
Comunicación y Consulta	Asistir a las partes interesadas a comprender el riesgo y obtener retroalimentación e información para apoyar la toma de decisiones.					X	
FASE VI: SEGUIMIENTO Y REVISIÓN							

Seguimiento y Revisión	Evaluar periódicamente la eficacia de la gestión del riesgo, registrar resultados, los cambios y proporcionar retroalimentación.			X			- El seguimiento normalmente se realiza con indicadores o métricas (KRIs)
FASE VII: REGISTRO E INFORME							
Registro e informe	Documentar e informar las decisiones de tratamiento, los resultados y las lecciones aprendidas.					X	

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	X

FIRMA DEL EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO EXPERTO

Datos Generales del Experto

Nombres y Apellidos: Oliver Vásquez Leyva

Grado Académico: Magister

Formación académica: Ingeniero de Sistemas.

Área de experiencia profesional: Gestión de TI.

Tiempo de experiencia: 13 años.

Cargo Actual: Jefe del Centro de Informática y Sistemas.

Institución donde labora: Universidad señor de Sipán.

Objetivo de la investigación: Proponer un modelo de gestión de riesgos de tecnologías de información basados en estándares adaptados en el sector de distribuidoras de la región Lambayeque para contribuir en la protección del activo de TI.

Objetivo de Juicio de Experto: Someter a consulta y validez el modelo de gestión de riesgos de TI aplicadas a empresas distribuidoras de artículos de ferretería, acabados y materiales de construcción de la región Lambayeque.

Escala de calificación: 1: Totalmente en desacuerdo 2: En desacuerdo 3: Ni de acuerdo ni en desacuerdo 4: De acuerdo 5: Totalmente de acuerdo. **Señale con X la opción elegida**

Sub Fase	Objetivo	ESCALA DE LIKERT					Observaciones
		1	2	3	4	5	
FASE I: ALCANCE, CONTEXTO Y CRITERIOS							
Alcance	Definir el alcance de las actividades de gestión del riesgo (estratégico, operacional, de programa, de proyecto)					X	
Contexto Internos	Comprensión del entorno interno de la organización.					X	
Contexto Externos	Comprensión del entorno externo en la organización.					X	
Criterio	Definición de los riesgos empresariales y su importancia como soporte para la toma de decisiones.					X	
FASE II: ANÁLISIS BIA							
Priorización de procesos y actividades	Definir los procesos y actividades críticas e importantes para continuidad y estabilidad de la organización.				X		Definir la continuidad y estabilidad de algunos proc
Análisis y consolidación	Realizar la consolidación de análisis del proceso BIA y los requisitos del negocio para su continuidad de operaciones.					X	

FASE III: EVALUACIÓN DEL RIESGO							
Identificación de activos	Identificar, clasificar y valorar los activos de TI, que dan soporte a la operatividad de la organización.					X	
Análisis del riesgo	Identificar las debilidades en la protección del activo (amenazas, vulnerabilidades, probabilidad e impacto).				X		
Valoración del riesgo	Valorar el riesgo respecto a los resultados obtenidos para su priorización y facilitar la toma de decisiones en la organización.					X	
FASE IV: TRATAMIENTO DEL RIESGO							
Estrategias de Tratamiento	Determinar la estrategia de tratamiento más apropiado para el rubro de la organización.					X	
Preparación e implementación de los planes de tratamiento del riesgo	Formular los planes de tratamiento del riesgo y especificar la manera en la que se implementarán las opciones elegidas para el tratamiento.					X	
FASE V: COMUNICACIÓN Y CONSULTA							
Comunicación y Consulta	Asistir a las partes interesadas a comprender el riesgo y obtener retroalimentación e información para apoyar la toma de decisiones.				X		
FASE VI: SEGUIMIENTO Y REVISIÓN							
Seguimiento y Revisión	Evaluar periódicamente la eficacia de la gestión del riesgo, registrar resultados, los cambios y proporcionar retroalimentación.					X	
FASE VII: REGISTRO E INFORME							
Registro e informe	Documentar e informar las decisiones de tratamiento, los resultados y las lecciones aprendidas.					X	

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	X

FIRMA DEL EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO EXPERTO

Datos Generales del Experto

Nombres y Apellidos: Jessie Leila Bravo Jaico

Grado Académico: Dra en ciencias de la Computación y Sistemas

Formación académica: Ing de Computación y Sistemas

Área de experiencia profesional: Gestión y Seguridad de la Información

Tiempo de experiencia: 25 años

Cargo Actual: Catedrática

Institución donde labora: UNPRG – USAT

Objetivo de la investigación: Proponer un modelo de gestión de riesgos de tecnologías de información basados en estándares adaptados en el sector de distribuidoras de la región Lambayeque para contribuir en la protección del activo de TI.

Objetivo de Juicio de Experto: Someter a consulta y validez el modelo de gestión de riesgos de TI aplicadas a empresas distribuidoras de artículos de ferretería, acabados y materiales de construcción de la región Lambayeque.

Escala de calificación: 1: Totalmente en desacuerdo 2: En desacuerdo 3: Ni de acuerdo ni en desacuerdo 4: De acuerdo 5: Totalmente de acuerdo. **Señale con X la opción elegida**

Sub Fase	Objetivo	ESCALA DE LIKERT					Observaciones
		1	2	3	4	5	
FASE I: ALCANCE, CONTEXTO Y CRITERIOS							
Alcance	Definir el alcance de las actividades de gestión del riesgo (estratégico, operacional, de programa, de proyecto)					X	
Contexto Internos	Comprensión del entorno interno de la organización.					X	
Contexto Externos	Comprensión del entorno externo en la organización.				X		
Criterio	Definición de los riesgos empresariales y su importancia como soporte para la toma de decisiones.					X	
FASE II: ANÁLISIS BIA							
Priorización de procesos y actividades	Definir los procesos y actividades críticas e importantes para continuidad y estabilidad de la organización.					X	
Análisis y consolidación	Realizar la consolidación de análisis del proceso BIA y los requisitos del negocio para su continuidad de operaciones.				X		

FASE III: EVALUACIÓN DEL RIESGO							
Identificación de activos	Identificar, clasificar y valorar los activos de TI, que dan soporte a la operatividad de la organización.					X	
Análisis del riesgo	Identificar las debilidades en la protección del activo (amenazas, vulnerabilidades, probabilidad e impacto).				X		
Valoración del riesgo	Valorar el riesgo respecto a los resultados obtenidos para su priorización y facilitar la toma de decisiones en la organización.					X	
FASE IV: TRATAMIENTO DEL RIESGO							
Estrategias de Tratamiento	Determinar la estrategia de tratamiento más apropiado para el rubro de la organización.					X	
Preparación e implementación de los planes de tratamiento del riesgo	Formular los planes de tratamiento del riesgo y especificar la manera en la que se implementarán las opciones elegidas para el tratamiento.				X		
FASE V: COMUNICACIÓN Y CONSULTA							
Comunicación y Consulta	Asistir a las partes interesadas a comprender el riesgo y obtener retroalimentación e información para apoyar la toma de decisiones.					X	
FASE VI: SEGUIMIENTO Y REVISIÓN							
Seguimiento y Revisión	Evaluar periódicamente la eficacia de la gestión del riesgo, registrar resultados, los cambios y proporcionar retroalimentación.				X		
FASE VII: REGISTRO E INFORME							
Registro e informe	Documentar e informar las decisiones de tratamiento, los resultados y las lecciones aprendidas.					X	

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	✓

FIRMA DEL EXPERTO

Anexo 9. Perfil de expertos

La información detallada a continuación ha sido obtenida del Directorio Concytec:

https://dina.concytec.gob.pe/appDirectorioCTI/

PERFIL DE EXPERTO	
	**Gilberto Carrión Barco** Doctor en Ciencias de la Computación y Sistemas. Maestro en Ingeniería de Sistemas, Magister en Docencia Universitaria. Ingeniero en Computación e Informática y Licenciado en Administración Pública, con Colegiatura N° 90931 por el Colegio de Ingenieros del Perú, habilitado. Con más de 12 años de experiencia en docencia universitaria en UNPRG, USS, UTP, USMP, USAT e Investigador en la línea Tecnologías de la Información, Gobierno Electrónico y Gestión por Procesos y Gestión por Resultados. Amplia experiencia como Jurado y Asesor de Investigaciones tanto en pregrado como en postgrado. Comprometido con el trabajo en equipo, proactivo y con vocación de servicio.

Datos Académicos

Grado	Título	Centro de Estudios
LICENCIADO / TÍTULO	INGENIERO EN COMPUTACION E INFORMATICA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
BACHILLER	BACHILLER EN COMPUTACION E INFORMATICA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
BACHILLER	BACHILLER EN ADMINISTRACIÓN PÚBLICA	UNIVERSIDAD SEÑOR DE SIPÁN
MAGISTER	MAESTRO EN INGENIERIA DE SISTEMAS, ESPECIALIDAD: CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
MAGISTER	MAGISTER EN DOCENCIA UNIVERSITARIA	UNIVERSIDAD PRIVADA CÉSAR VALLEJO
DOCTORADO	DOCTOR EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD SEÑOR DE SIPÁN

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DOCENTE ORDINARIO TIEMPO COMPLETO CATEGORÍA AUXILIAR	2008-08-01	A la actualidad
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECTOR DE ESCUELA	2013-12-01	2016-01-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE AREA ADMINISTRATIVA RED TELEMÁTICA	2010-07-01	2011-11-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DE LABORATORIO	2010-04-01	2010-09-01
INSTITUTO DE EDUCACION SUPERIOR TECNOLOGICO PRIVADO ABACO	GERENTE DE ALTA TECNOLOGÍA E INNOVACIÓN TECNOLÓGICA	2004-03-01	2006-01-01

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD TECNOLOGICA DEL PERU S.A.C. O UTP S.A.C.	Ordinario-Auxiliar	Mayo 2014	A la actualidad
UNIVERSIDAD DE SAN MARTIN DE PORRES	Ordinario-Auxiliar	Agosto 2010	Noviembre 2016
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Auxiliar	Agosto 2008	A la actualidad
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Ordinario-Auxiliar	Agosto 2006	Diciembre 2009
UNIVERSIDAD SENOR DE SIPAN SAC	Ordinario-Asociado	Abril 2006	A la actualidad

Experiencia como asesor de tesis

Universidad	Tesis	Tesistas	Fecha aceptación
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Magister	Rosa America Cobeñas Sanchez	Noviembre 2016

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Guevara Chumán, Javier Gustavo	Agosto 2015
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Rivas Estrada, Carol Meliza; Estrada Masgo, Danny Christian	Junio 2014
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Arévalo Diaz Janira; Sánchez Pérez Cinthya del Milagro	Febrero 2015
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ramírez Arrunátegui Pamela Susanne; Rojas Muñoz Jonatan Jorge	Abril 2015
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Apolaya Segura Carlos Eduardo; Vilchez Castillo Sylvía Susana	Junio 2018
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Palacios Ormeño, Julio César	Noviembre 2013
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Arrieta Gómez, Víctor Manuel; Camacho Aguirre, Martin Horacio	Julio 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Villegas Carrasco, Carlos Alonso; Negreiros Chinchihuara, Wilfredo Martin	Octubre 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Sacravilca Narciso, Dante Gonzalo; López Alarcón, Absalón	Junio 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Balcazar De Los Santos, César Augusto; Correa Villegas, Ricardo	Octubre 2013

PERFIL DE EXPERTO

CELI AREVALO ERNESTO KARLO

Experiencia docente y de investigación desde 1994. He desarrollado trabajos de investigación de manera individual y conformando equipos de trabajo multidisciplinarios. Las áreas de interés de mis investigaciones están relacionadas con el uso, aplicación o desarrollo de tecnologías de la información, como: - infraestructura de TI en hospitales: sistemas HIS y sistemas de administración de imágenes médicas - RIS PACK - uso de las TIC en los procesos enseñanza aprendizaje: síncronos y asíncronos - ingeniería de software e ingeniería de la información: métodos de desarrollo, modelado de procesos, modelado de datos, métricas, ciclo de vida - base de datos: métodos de ordenamiento y búsqueda - Modelos de gestión de riesgos de TI: análisis y tratamiento de riesgos - Modelos para auditorías informáticas - Tableros de mando para control y seguimiento de procesos

Datos académicos

Grado	Título	Centro de Estudios
DOCTORADO	DOCTOR EN ADMINISTRACION	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
MAGISTER	MAESTRO EN CIENCIAS, ESPECIALIDAD: INFORMATICA Y SISTEMAS	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
LICENCIADO / TÍTULO	INGENIERO DE COMPUTACION Y SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO
BACHILLER	BACHILLER EN INGENIERIA DE COMPUTACION Y	UNIVERSIDAD PRIVADA ANTENOR ORREGO

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
NIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECTOR DE ESCUELA	2016-01-01	A la actualidad

CAJA RURAL DE AHORRO Y CREDITO CRUZ DE CHALPON (HOY CAJA SIPAN)	AUDITOR EXTERNO DE TI	2002-10-01	2015-12-01
CONSORCIO ATA - KUKOVA	PROYECTISTA PRINCIPAL	2009-11-01	2011-08-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DECANO	2008-07-01	2011-07-01
CONSORCIO ATA - KUKOVA	PROYECTISTA PRINCIPAL	2009-12-01	2011-04-01
MUNICIPALIDAD PROVINCIAL CONDORCANQUI	LIDER DE PROYECTO	2006-06-01	2006-11-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECTOR DE ESCUELA	2001-04-01	2006-09-01
MINISTERIO DE LA PRODUCCION	ANALISTA DE PROCESOS	2004-07-01	2005-07-01
PROYECTO ESPECIAL OLMOS TINAJONES	SUPERVISOR DE ELABORACION DE EXPEDIENTE TECNICO	2002-04-01	2002-11-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DE OFICINA CENTRAL	2001-05-01	2001-12-01

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD DE LAMBAYEQUE SAC	Contratado	Marzo 2012	Julio 2017
UNIVERSIDAD SENOR DE SIPAN SAC	Contratado	Setiembre 2011	Diciembre 2011
UNIVERSIDAD SENOR DE SIPAN SAC	Contratado	Abril 2002	Diciembre 2004
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Principal	Octubre 1994	A la actualidad

Investigaciones

Tipo de Producción	Título	Descripción	Fecha Inicio	Fecha Fin	Área Principal
ARTÍCULO EN REVISTA CIENTÍFICA	Application of Dashboards and Scorecards for Learning Models IT Risk Management: A User Experience	Design, User Experience, and Usability - Interactive Exp...	2015	2015	Ingeniería y Tecnología
ARTÍCULO EN REVISTA CIENTÍFICA	Modelo de gestión de riesgos operativos de TI y de la continuidad de los procesos académicos-administrativos críticos, como parte de la gestión de incidentes de la seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo	El objetivo es evaluar los riesgos asociados a los procesos principales de la UNPRG, con la finalidad de identificar y cuantificar los niveles de riesgos a los que está expuesto, que pudieran ´paralizar dichos procesos, proponiendo los controles necesarios para mitigarlos utilizando como referencia la norma ISO/IEC 27001	Junio 2013	Marzo 2014	Ingeniería y Tecnología
LIBRO	Auditoria de sistemas		2002	2002	Ingeniería y Tecnología

PERFIL DE EXPERTO

Oliver Vásquez Leiva

Experiencia docente en las ciencias de la educación, ingeniería de sistemas, administración y gestión de empresas en los sectores de la ingeniería, producción y comercialización. La práctica de la mejora continua, manejo de estándares en calidad, responsabilidad social, conciencia medioambiental y la gestión procesos serán requisitos básicos en la formación y práctica profesional del siglo. Por lo que nuestro reto es trasladar la experiencia al servicio de equipos de trabajo y estudiantes.

Datos académicos

Grado	Título	Centro de Estudios
MAGISTER	MAGISTER EN ADMINISTRACION ESTRATEGICA DE EMPRESAS	PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU
LICENCIADO / TÍTULO	LICENCIADO EN EDUCACION, ESPECIALIDAD: MATEMATICA Y COMPUTACION	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
BACHILLER	BACHILLER EN EDUCACION	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
MAGISTER	MAESTRO EN CIENCIAS DE LA EDUCACION , ESPECIALIDAD: CON MENCION EN INVESTIGACION Y DOCENCIA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
LICENCIADO / TÍTULO	INGENIERO DE SISTEMAS	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
LICENCIADO / TÍTULO	LICENCIADO EN ADMINISTRACIÓN	UNIVERSIDAD SEÑOR DE SIPÁN
BACHILLER	BACHILLER EN INGENIERIA DE SISTEMAS	UNIVERSIDAD SEÑOR DE SIPÁN
BACHILLER	BACHILLER EN ADMINISTRACIÓN	UNIVERSIDAD SEÑOR DE SIPÁN

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
UNIVERSIDAD SENOR DE SIPAN SAC	DIRECTOR DEL CENTRO DE INFORMÁTICA Y SISTEMAS	2013-12-01	A la actualidad
SOLTI SOCIEDAD ANÓNIMA CERRADA	GERENTE	2012-12-01	A la actualidad

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD CESAR VALLEJO S.A.C.	Contratado	Marzo 2016	A la actualidad
UNIVERSIDAD SENOR DE SIPAN SAC	Contratado	Marzo 2008	Mayo 2016

Experiencia como asesor de tesis

Universidad	Tesis	Tesista(s)	Fecha Aceptación
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	ARTEAGA MONTALVO KARLA YAMILI	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	ASTOLINGON NUÑEZ ARELY ESTER	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	CHAMBERGO ANACLETO DAVID	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	CHANAME MORI OLGA LUISA	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	CRIOLLO LLACSAHUANGA LIZETH	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	FERNANDEZ PINEDO ELIZABETH	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	GUZMAN LLUEN JHOANNA LORENA	Noviembre 2016

UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	HUILCA MORI KATHERINE MICHELLE	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	JAVA DURAN LUZ AURORA	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	JIMENEZ RIVERA MILAGROS	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	MEREGILDO SALVADOR CINTHIA MABEL	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	MUÑOZ MARTINEZ JOAO JOSIMAR	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	NAVARRO HEREDIA GIAN CARLOS	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	PEREZ RUIZ RAQUEL JACQUELINE	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	RODRIGUEZ FLORES ANTHONY GIAMPIERRE	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	ROJAS DURAN VIOLETA DEL ROCIO	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	SALAZAR LLUEN IVONNE JHOSSELIN	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	SANCHEZ MONTENEGRO MILAGROS	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	SEGURA GOMEZ SONIA AZUCENA	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	VASQUEZ SALDAÑA QUIN ROY JEFERSSON	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	VERA CAVA OSMAR ALEJANDRO	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO	Bachiller	YAIPEN MIMBELA JONATHAN	Noviembre 2016

S.A.C.		JAVIER	
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	ZAVALA SIALER YASMIN STHEFANY	Noviembre 2016
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	HURTADO CHERO ARTURO JESÚS	Noviembre 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	SAAVEDRA CARBAJAL JUAN CARLOS	Enero 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	ZEVALLOS LLONTOP VICTOR ENRIQUE	Mayo 2015
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	SALAZAR GUEVARA LENIN JESUS	Abril 2015
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	ALFARO ESQUIVEL LUZ MARIA	Abril 2015
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	ESPINOZA PASTOR CESAR RAYMUNDO	Diciembre 2011

PERFIL DE EXPERTO

Jessie Leila Bravo Jaico

Ing. de Computación y Sistemas. Primera Promoción de la Universidad Privada Antenor Orrego de Trujillo. Doctora en Ciencias de Computación y Sistemas en la USS. Magister en Informática y Multimedia en la Universidad de Los Lagos - Chile. Magister en Administración de empresas con mención en Gerencia Empresarial de la Universidad Nacional Pedro Ruiz Gallo. Especialización en Redes Informáticas, Gestión de proyectos, Auditoría y consultoría de sistemas. Asesora y Consultora de TI en empresas de la región.

Datos Académicos

Grado	Título	Centro de Estudios
MAGISTER	MAGÍSTER EN INFORMÁTICA Y MULTIMEDIA	UNIVERSIDAD SAN PEDRO
LICENCIADO / TÍTULO	INGENIERO DE COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO
BACHILLER	BACHILLER EN INGENIERIA DE COMPUTACION Y SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO
MAGISTER	MAESTRA EN ADMINISTRACION CON MENCION EN GERENCIA EMPRESARIAL	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
DOCTORADO	DOCTORA EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD SEÑOR DE SIPÁN

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
SERVIMEDICOS S.A.C.	CONSULTORA TI	2006-06-01	2008-09-01
INSTITUTO DE ALTA CALIDAD DE ATENCION A LA SALUD EN LIQUIDACION	CONSULTORA TI	2005-04-01	2007-07-01

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DEL LABORATORIO DE CÓMPUTO	2003-09-01	2006-12-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DEL LABORATORIO DE CÓMPUTO	2001-05-01	2003-09-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DESARROLLO SISTEMAS	1996-06-01	2000-12-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECCIÓN DE ESCUELA	1997-09-01	1999-12-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	MIEMBRO COMITÉ DIRECTIVO	1996-12-01	1999-12-01
CIS - CATSOFT S.R.LTDA.	ANALISTA-DISEÑADORA	1996-09-01	1997-12-01
CUERPO MÉDICO HOSPITAL NACIONAL ALMANZOR AGUINAGA ASENJO	PROGRAMADORA	1993-01-01	1993-03-01

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Principal	Junio 2010	A la actualidad
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Contratado	Agosto 2002	A la actualidad
UNIVERSIDAD JUAN XXIII-VALLE JEQUETEPEQUE	Contratado	Agosto 1999	Diciembre 2000
UNIVERSIDAD SAN PEDRO	Contratado	Setiembre 1998	Diciembre 1999
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Auxiliar	Mayo 1998	Diciembre 2001
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Contratado	Octubre 1994	Abril 1998

Experiencia como asesor de tesis

Universidad	Tesis	Tesista(s)	Fecha Aceptación
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	CÉSAR WENCESLAO DE LA CRUZ GUERRERO y JUAN CARLOS VASQUEZ MONTENEGRO	Abril 2008
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	Santa Maria Becerra, Franck Jhonathan	Junio 2012
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	BURGA BASTO, JORGE HUMBERTO JESÚS y LEY CUÉN RODAS, CHRISTIAN ALEXIS	Abril 2011
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	RICHARD TUSET TRINIDAD y DANIEL ALEJANDRO YI RAMOS	Abril 2011
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	César Augusto López Nicolini	Junio 2014
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Fernández Vílchez Richar Marvin	Enero 2012
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	ALARCÓN CUSMAN JOSÉ CARLOS y CHERO IZQUIERDO JULIO FRANCISCO	Mayo 2014
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Roxana Paola Bazan becerra	Febrero 2001
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	María del Rosario Becerra Aguilar	Setiembre 2002
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Guisella Lontop Vilchez/Franklin Terán/Melvy terán	Junio 2003
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Milagros Vanessa Peña Seclén/Monica Lecca Vinces	Abril 2004

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ronald Javier Medina Campaña	Abril 2006
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	CHANAME BALDERA, OSCAR ENRIQUE	Abril 2006
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Chirinos Fernandez Maykol	Julio 2007
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ronald Leiva Peña	Febrero 2016
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	GONZALO MARTIN ROMERO ABANTO y ROBERTH CÓRDOVA OBLITAS	Noviembre 2017
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Olano Díaz, Juan Daniel; Sánchez Aguilar, Segundo Román	Marzo 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Pérez Artemio, Calderón; Vásquez Hoyos, Alvaro	Julio 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Cubas Penas, Clara Patricia	Abril 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Magister	Niño Morante, Nilton Rogger	Mayo 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Arenas Morales, Victor Jaime / Brios Guevara, Lessly Yein	Marzo 2019
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	LARREA DUPIS CARLO ANTONIO / HERNÁNDEZ CAMPOS ROBERT DANILO	Marzo 2019