MODELAMIENTO DE PROCESOS BASADOS EN EL GRUPO DE NORMAS INTERNACIONALES ISO/IEC 27000 PARA GESTIONAR EL RIESGO Y SELECCIONAR CONTROLES EN LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

ING. ELKIN REINA GARCÍA

ING. JOSÉ RAÚL MORALES RAMÍREZ

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y CIENCIAS DE LA COMPUTACIÓN

PROGRAMA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

ESPECIALIZACIÓN EN REDES DE DATOS

PEREIRA

2014

MODELAMIENTO DE PROCESOS BASADOS EN EL GRUPO DE NORMAS INTERNACIONALES ISO/IEC 27000 PARA GESTIONAR EL RIESGO Y SELECCIONAR CONTROLES EN LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

ING. ELKIN REINA GARCÍA

ING. JOSÉ RAÚL MORALES RAMÍREZ

PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE

ESPECIALISTA EN REDES DE DATOS

DIRECTORA PROYECTO

ANA MARÍA LÓPEZ ECHEVERRY

INGENIERA ELECTRICISTA

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y CIENCIAS DE LA COMPUTACIÓN

PROGRAMA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

ESPECIALIZACIÓN EN REDES DE DATOS

PEREIRA

2014

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Pereira, noviembre de 2014

Dedicado a nuestras familias quienes con su incondicional apoyo han hecho posible alcanzar este nuevo logro.

AGRADECIMIENTOS

A Dios, por la oportunidad de alcanzar esta meta gratificante tanto personal como familiarmente.

Al Grupo de Investigación Nyquist por permitirnos hacer parte en el desarrollo del proyecto Macro como aporte a la competitividad de las empresas de la región.

A la ingeniera Ana María López Echeverry, por toda su colaboración y disposición en la dirección de este proyecto.

A la ingeniera Paula Andrea Villa, compañera de estudio, por el apoyo en temas importantes del proyecto.

…

CONTENIDO

pág.

Índice de Figuras

Índice de Cuadros

I. INTRODUCCIÓN

En la búsqueda de la competitividad empresarial, es indispensable para cualquier compañía garantizar que sus procesos de gestión de la información sean lo suficientemente efectivos, confiables y organizados, de tal manera que se pueda prestar un servicio o entregar un producto con calidad. Para esto las compañías deben valerse de las metodologías y modelos aprobados internacionalmente que promueven una gestión de la información con seguridad, haciéndose indispensable implementar los procesos y procedimientos necesarios para alcanzar este objetivo.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es una herramienta que le permite a una compañía realizar una completa gestión de los riesgos que se presentan en la producción, procesamiento, almacenamiento y análisis de la información, buscando mantener siempre las características de Confidencialidad, Integridad y Disponibilidad con las que esta debe contar. La implementación de un SGSI en cualquier compañía conlleva realizar una serie de actividades que deben ceñirse a lo señalado por el grupo de normas ISO/IEC 27000, siendo la ISO/IEC 27001 la que establece los requisitos para la certificación, pero teniendo en cuenta las recomendaciones y mejores prácticas descritas en las demás.

Como una parte del proyecto denominado ***"Sistema de gestión de seguridad soportado en TIC para realizar un aporte a la competitividad de las empresas de la región"*** presentado ante Colciencias por el grupo de investigación Nyquist de la Universidad Tecnológica de Pereira, se desarrolla este proyecto con el fin de brindar a las empresas de la región unas guías que permitan interpretar más claramente lo que se menciona específicamente en el capítulo SGSI de la norma ISO/IEC 27001, en lo referente a la gestión de los riesgos, abordando todas sus etapas y guiando claramente los pasos para la correcta implementación del sistema de gestión, de tal manera que se termine describiendo el ***Cómo*** hacer lo solicitado en esta norma.

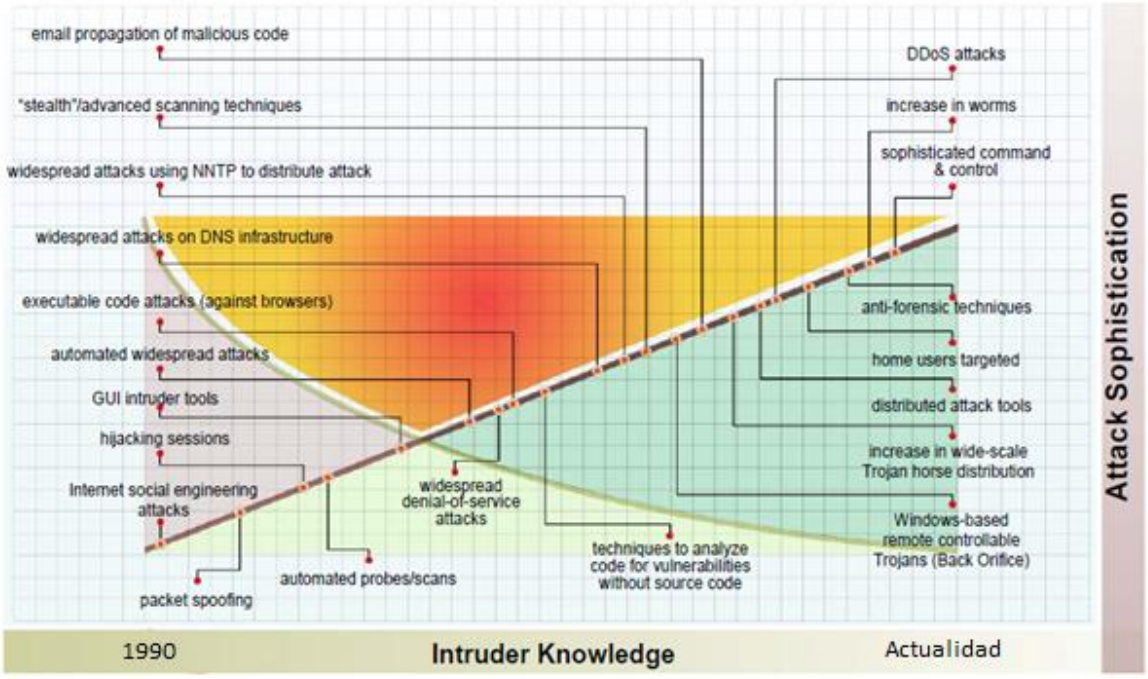
2. DEFINICIÓN DEL PROBLEMA

A diario el negocio de las compañías está amenazado por riesgos internos y externos que ponen en peligro la integridad de la información y por lo tanto su éxito y competitividad. El cibercrimen y ciberterrorismo hoy día son amenazas latentes que algunos ven muy lejanas y que se cree no afectan las empresas de la nación o de la región.

En la actualidad es relativamente fácil para una persona tener acceso a herramientas informáticas que le permiten acceder a información confidencial de una organización ya que generalmente ésta permanece en sistemas de información como equipos y/o dispositivos de almacenamiento y es transmitida por redes de datos e internet. Los avances tecnológicos, la facilidad de uso, disponibilidad en el mercado y la alta capacidad de cómputo de los equipos informáticos han contribuido a la globalización de la economía y por lo tanto a realizar negocios de distintas formas ya no tradicionales, como por ejemplo compras en tiendas virtuales o comercio electrónico, realizados inclusive entre países lejanos y de diferentes culturas alrededor del planeta. Sin embargo, esta situación y sus características también han facilitado que se presenten ataques hacia la información corporativa, ya que aprovechando sus bondades, los ataques son materializados de una forma más sofisticada y cada vez exigen menor conocimiento del atacante gracias a las herramientas disponibles para este fin.

Esta relación se puede observar en la figura 1.

Figura 1: Relación entre sofisticación y conocimiento del atacante[1]



Así las cosas, los riesgos a los que se expone hoy día una organización son nuevos y más complejos, inclusive se puede dar el caso de sabotear el funcionamiento de un estado atacando sus diferentes frentes y fuentes de información. Un claro ejemplo de esto se dio para la primera vuelta de las elecciones presidenciales en Colombia efectuadas el 30 de mayo de 2010; el entonces ministro de defensa Gabriel Silva Luján denunció un plan de piratas informáticos para sabotear el conteo de votos así como para atacar la estructura informática del país. "En el mundo cibernético no hay fronteras y los intereses terroristas no tienen fronteras, desafortunadamente cuando se trata de atacar al país también en su estructura informática", dijo Silva en declaraciones a periodistas. "Hemos detectado que hay esfuerzos de 'hackers' de otros países y en otras jurisdicciones que están buscando afectar no solo la Registraduría y el día de las elecciones, sino penetrar y afectar la seguridad informática del país"[2], precisó.

[1]Allen Julia H. Information Security as an Institutional Priority [En línea] <http://www.cert.org/archive/pdf/info-sec-ip.pdf>, [Consultado 14 de Diciembre de 2013]

[2] Revista América Económica, Política y Sociedad [En línea] <http://www.americaeconomia.com/politica-sociedad/politica/colombia-advierte-sobre-riesgo-de-ataque-informatico-durante-elecciones> [Consultado 14 de Diciembre de 2013]

Otro ejemplo de ataques informáticos que ha sufrido el país, según se publicó en el año 2012, los ataques de la organización activista Anonymous dejaron fuera de servicio las páginas web del Ministerio del Interior y de Justicia, el Senado y la Presidencia de la República, Gobierno en Línea y Ministerio de Defensa, lo cual evidenció incapacidad en la ciber-defensa nacional para enfrentar este tipo de amenazas obligando al gobierno a generar lineamientos de una política de ciber seguridad y ciber defensa y la creación del ColCERT – Equipo de Respuestas a Emergencias Informáticas de Colombia, dependiente del Ministerio de Relaciones Exteriores[3].

Otros riesgos corresponden a la delincuencia organizada cuyo fin es lucrativo por medio de robo de información, espionaje industrial, suplantación de tarjetas de crédito, manipulación o alteración de información, acceso a información confidencial y robo de cuentas bancarias en forma masiva; situaciones que son más comunes en nuestro medio. Todo lo anterior puede tener orígenes tanto internos como externos, es decir, empleados propios y/o clientes, proveedores, agentes particulares, etc.

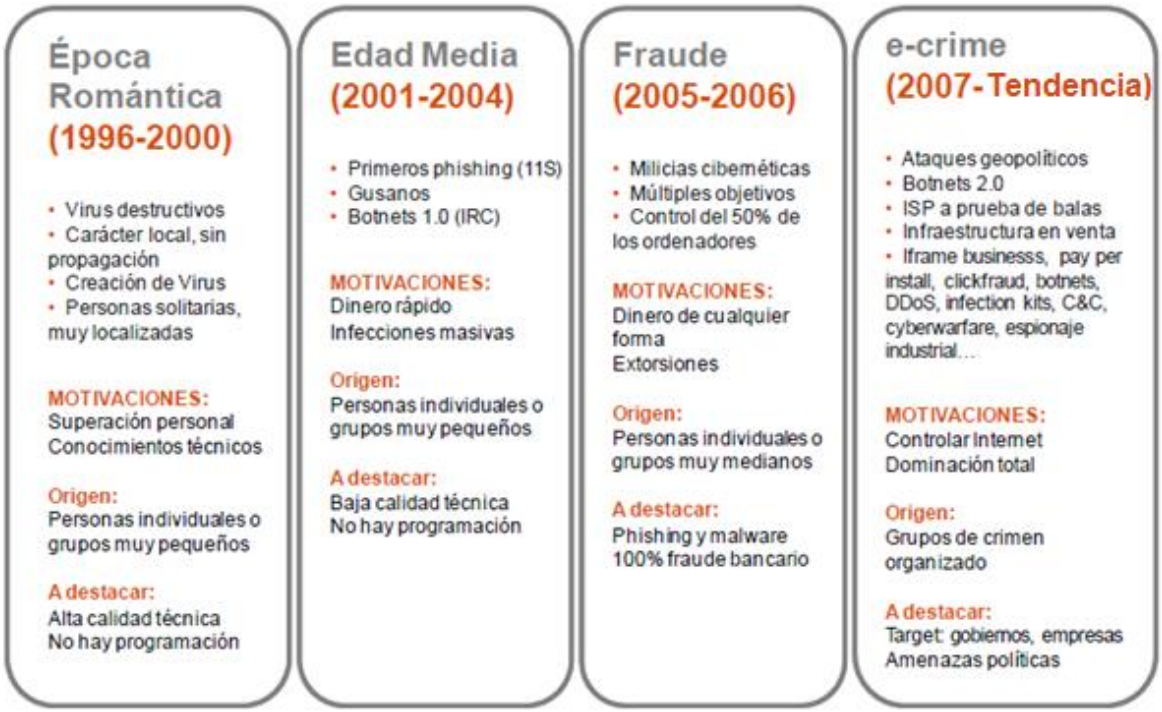
La compañía S21sec es una empresa especializada en servicios de seguridad digital, fue fundada en el año 2000 y es miembro del ***Consejo Nacional Consultor sobre Cyber Seguridad (CNCCS),*** una organización privada que tiene como miembros a Panda Security, S21sec, Hispasec Sistemas, SecuwareCybex, Amper, Telefónica, TBSecurity, Barcelona Digital Centro Tecnológico, Universidad de Deusto Laboratorio S3Lab, Colegio Oficial de Ingenieros de Telecomunicación (COIT) y AEDEL[4]. Su misión es poner a disposición de las diversas organizaciones que operan en España, gubernamentales o no, el conocimiento y experiencia de sus miembros en asuntos relacionados con la ciber-seguridad nacional o global, con el fin de hacer más segura Internet y las redes de Información.

Estudios realizados por S21sec muestran la evolución de los ataques y sus motivaciones.

[3] Ciberseguridad: Colombia ante un ataque. 2012. [En línea]. <www.gerente.com/detarticulo.php?CodArticl=385> [Consultado junio de 2013]

[4] Informe anual de fraude Online y Cibercrimen 2012, [En línea] <http://www.s21sec.com/descargas/informe_anual_fraude_2009.pdf> [Consultado 14 de Diciembre de 2013]

Figura 2: Evolución del cibercrimen[5].

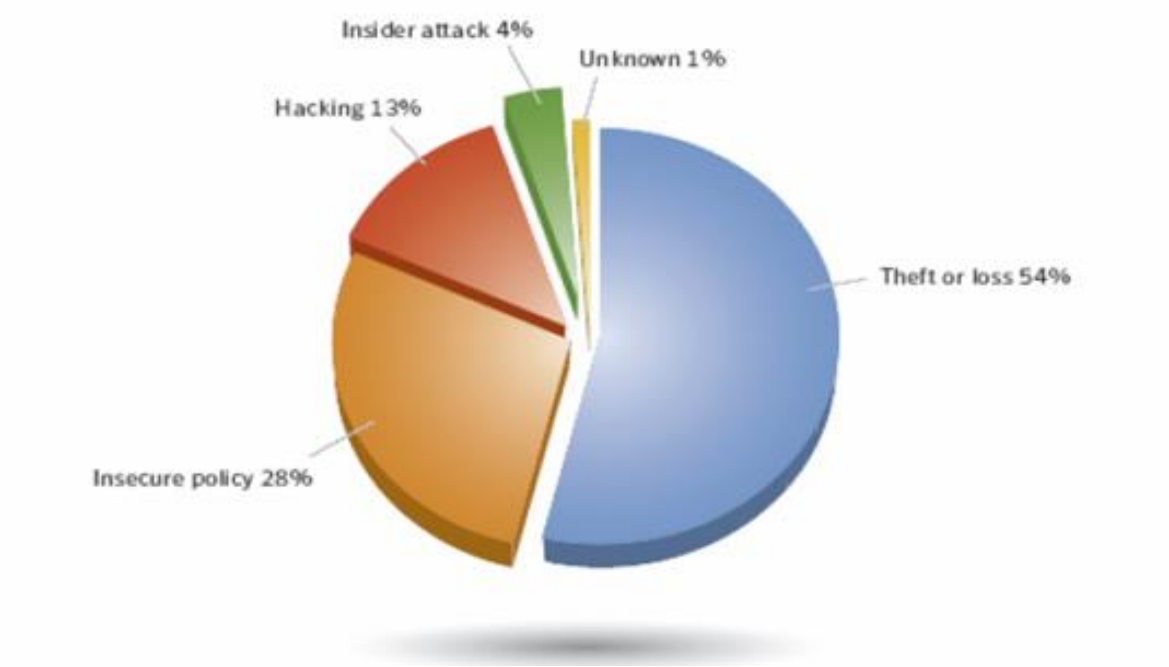


El estudio realizado por esta compañía muestra que no hay cambios sustanciales en las amenazas a la seguridad de la información, pero sí hay aumento del ritmo de ocurrencia de los incidentes de seguridad usando las mismas herramientas. Llama la atención la innovación en los delitos por internet donde las bandas organizadas buscan sacar el mayor provecho económico a sus acciones y concluye que se convierte en un riesgo mayor a empresas que no son objetivos de estos ataques pero sí las utilizan apoderándose de sus equipos de cómputo para lograr sus objetivos. Estas empresas "víctimas" pueden estar ubicadas incluso a nivel mundial y en países lejanos al de origen del ataque. También resalta el ataque a las personas con el fin de deshabilitar los controles de seguridad para el acceso a la red de la compañía, esto es más fácil que atacar los sistemas de seguridad. Por último destaca el descubrimiento de nuevas vulnerabilidades a las aplicaciones, protocolos de comunicaciones, sistemas operativos, equipos de cómputo y controles que hace prever nuevos ataques. En otra línea de problemas se hicieron públicos algunos métodos para descifrar comunicaciones GSM.

[5] Informe anual de fraude Online y Cibercrimen 2012, [En línea]<www.s21sec.com> [Consultado 14 de Diciembre de 2013]

Como se muestra en la figura 3, los ataques provienen de diferentes fuentes: ataques internos, mercados emergentes (pobre cooperación internacional), herramientas de colaboración (ej. blogging), software robots, malware en dispositivos móviles.

Figura 3: Orígenes de los ataques[6].



Como se mencionó anteriormente, hay riesgos internos y externos asociados a vandalismo o sabotaje como hackers, robos de identidad, spam, virus y espionaje entre otros, pero también afectan la información los riesgos físicos como incendios, inundaciones, terremotos, etc. Todos los anteriores impactan los tres principios del manejo de la información: ***Confidencialidad, Integridad y Disponibilidad*** y por supuesto la continuidad del negocio.

Es importante diferenciar entre la seguridad informática y la seguridad de la información. La primera es la protección de la infraestructura tecnológica y la segunda hace referencia a los activos de información confidenciales que hacen valer la compañía y dan su éxito en el mercado, por ejemplo bases de datos, contratos, actas, etc; es decir, esto se considera un activo tan importante para la

[6] IBM Report: Surge in CRIMINAL-DRIVEN CYBER ATTACKS [En línea] <https://www-03.ibm.com/press/us/en/pressrelease/19141.wss> [Consultado 26 de marzo de 2012]

organización así como recurso humano, maquinaria, muebles y enseres, utilidades, entre otros. Su presentación puede ser de manera física o digital y debe tenerse en cuenta que tiene un ciclo de vida ya que los planes estratégicos pueden hacer que pierda vigencia.

La mejor manera para que una compañía opere de forma segura es proteger sus datos claves con la ayuda de un ***Sistema de Gestión de Seguridad de la Información (SGSI)***. Este sistema está basado en procesos, es decir en gestión de actividades por parte de cada uno de los integrantes de la organización para transformar una entrada en un resultado propio de cada área de tal manera que permita identificar, tratar y minimizar los riesgos que atenten contra la información del negocio y por supuesto establecer las medidas de seguridad necesarias y controles que permiten medir la eficacia de tales medidas. Este sistema es preventivo ya que permite anticiparse a los problemas y prepararse ante cualquier incidente de seguridad.

Esta problemática no es ajena a la región. En una entrevista concedida a este grupo por el Ingeniero José Albeiro Rodríguez Patiño, gerente de la empresa C&C Consultores domiciliada en Pereira y con alta experiencia en sistemas de calidad, en la región han sido pocas las empresas que han mostrado interés para implementar un SGSI.

El ingeniero José Albeiro manifiesta que gracias a la masificación de internet, a la competitividad y globalización económica es común la exposición a varios tipos de riesgos que afectan la información y continuidad del negocio en las compañías locales, por ejemplo malware, virus, spam, sabotaje, suplantación, robo y filtración de información, ingeniería social, fallas eléctricas, fallas en las copias de seguridad y restauraciones, inundaciones, entre otros.

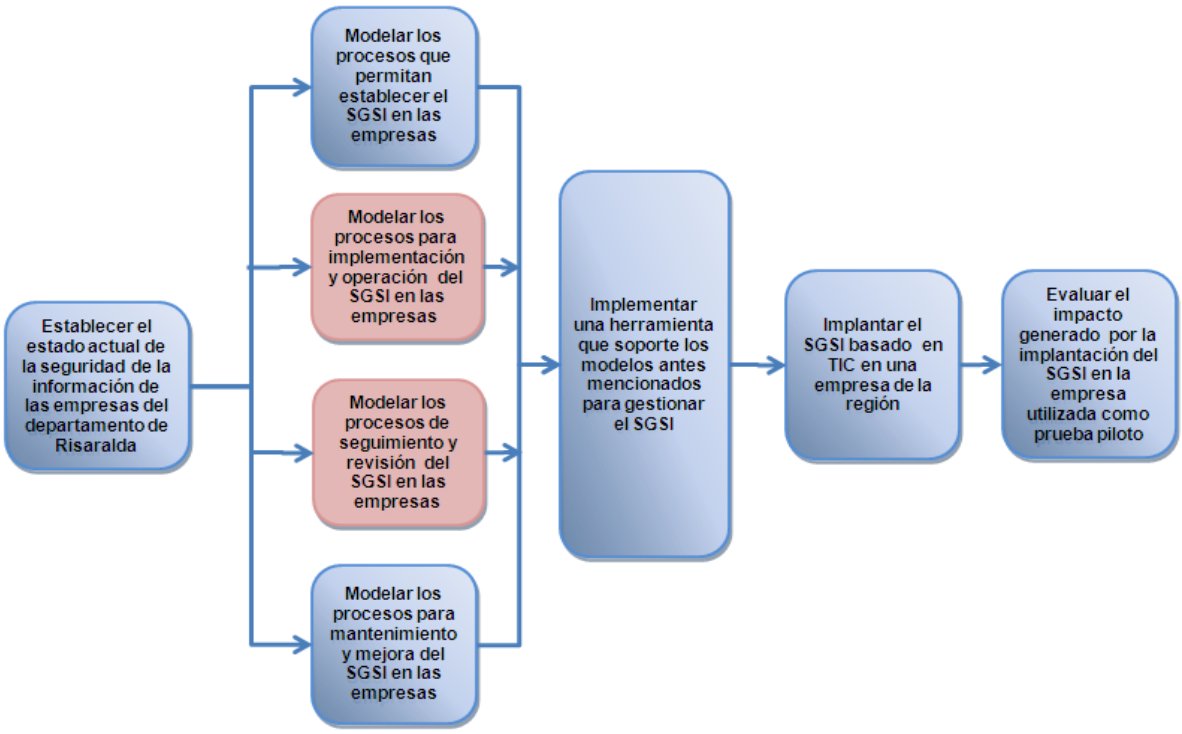
Lo anterior indica que gran parte de las empresas regionales no cuentan con modelos de los procesos para hacer tratamiento de riesgos, trazar objetivos de control, establecer controles y realizar una medición de la eficacia de tales controles que permita cumplir los requisitos de seguridad y proteger los activos de información. Sentida esta necesidad, se plantea este proyecto para que sirva de guía a las organizaciones regionales y así modelar metodológicamente sus procesos relacionados con estos aspectos.

Este es un trabajo derivado de un proyecto macro llamado ***“Sistema de gestión de seguridad soportado en TIC para realizar un aporte a la competitividad de***

las empresas de la región" a cargo del grupo de investigación Nyquist de la Universidad Tecnológica de Pereira, liderado por la Ing. Ana María López Echeverry y que será desarrollado en varias etapas por estudiantes de pregrado y posgrado.

El proyecto expuesto en este documento se orienta a modelar los procesos de tratamiento de riesgos y selección de objetivos de control y controles tratados en la norma ISO/IEC 27001 capitulo SGSI, en las secciones 4.1-Requisitos Generales, 4.2.1-Establecimiento y Gestión, 4.2.2-Implementación y Operación, 4.2.3-Seguimiento y Revisión y 4.2.4-Mantenimiento y Mejora del SGSI. Como se ve en la figura 4, el proyecto macro consta de varios módulos los cuales aún no están desarrollados. Este trabajo busca implementar específicamente las etapas "Modelar los procesos para la implementación y operación del SGSI en las empresas" y "Modelar los procesos de seguimiento y revisión del SGSI en las empresas".

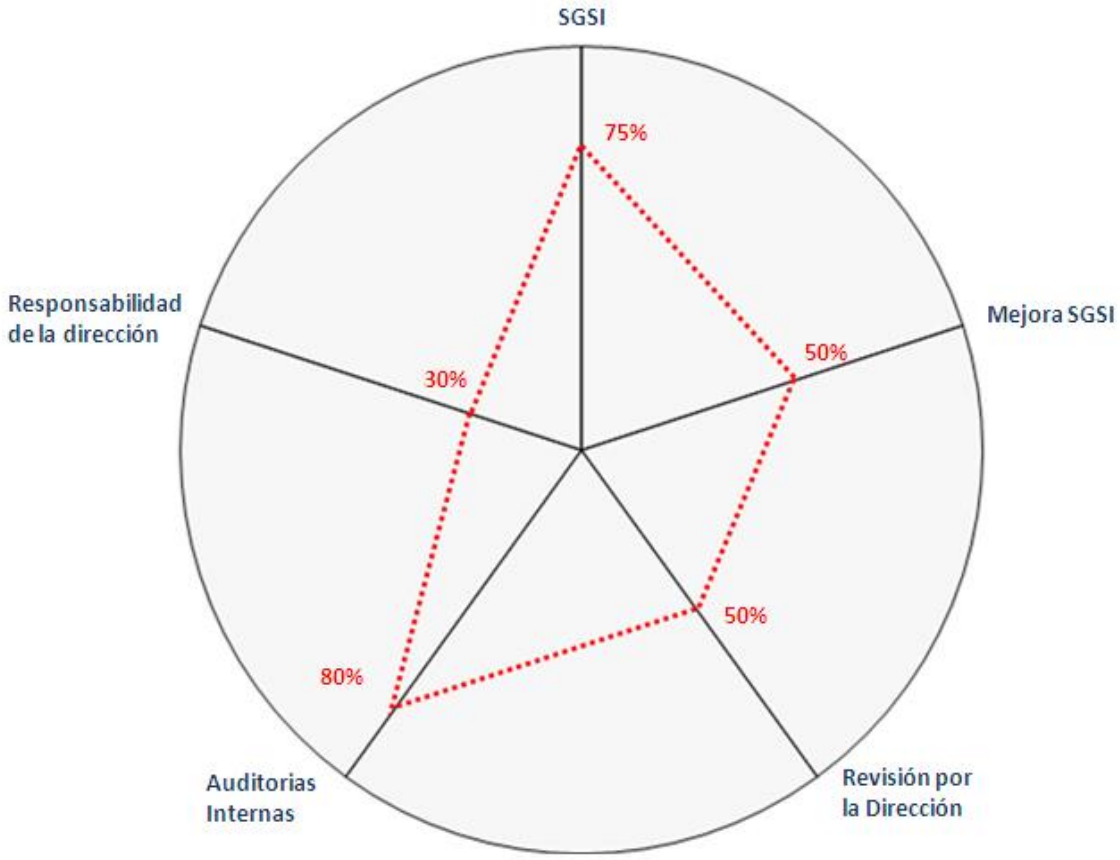
Figura 4: Módulos del proyecto Sistema de gestión de seguridad soportado en TIC para realizar un aporte a la competitividad de las empresas de la región.[7]



[7] Villa Sánchez, Paula A. Definición de procesos de auditoría interna del sistema de gestión de seguridad de la información soportado en TIC. Pereira (Rda). Universidad Tecnológica de Pereira, 2011.

Como lo demuestra la figura 5, el análisis paso a paso de los requerimientos de la norma y la elaboración de una gráfica a escala de cumplimiento de los cinco requisitos exigidos por la norma ISO/IEC 27001, brindará una idea de qué tan avanzado se encuentra el SGSI y permitirá determinar si la previsión de recursos y compromiso de la alta dirección están al nivel exigido.

Figura 5: Análisis paso a paso ISO/IEC 27001[8].



[8] Norma Técnica Colombiana NTC-ISO/IEC 27001.

3. JUSTIFICACIÓN

Cualquier empresa, sin importar su naturaleza, número de empleados, ubicación geográfica, etc. realiza actividades similares como procesar información, clasificarla como confidencial y por lo tanto protegerla; se expone a riesgos de seguridad y riesgos físicos y hacen alguna gestión al respecto. Se parte de la premisa de que la información es tal vez el activo más valioso de una organización. La información puede ser almacenada en diferentes formas como física, digital e incluso se considera el conocimiento como parte de ésta.

La información puede ser transmitida de diferentes formas incluyendo verbalmente. De una forma espontánea y descuidada podemos exponer este activo con las actividades diarias, contratos, cotizaciones, acuerdos de niveles de servicio, llamadas telefónicas, correo electrónico, reuniones con particulares, tratamiento de temas internos en áreas públicas, manejo de impresiones y papel reciclable, copia de correos electrónicos a personas no relacionadas con el tema aunque haga parte de la compañía entre muchas otras. Estas situaciones se presentan sirviéndose también de la tecnología, computadores, servidores, aplicaciones, internet, etc.

Las organizaciones poseen información que se debe proteger ante todo riesgo y amenaz; esto es un activo. Una amenaza es un evento o incidente de seguridad que aprovecha una debilidad o vulnerabilidad y que afecta los activos. Exponer un activo a que una amenaza se materialice conlleva a riesgos que podrían afectar el buen desempeño de la organización. En un proceso de gestión y tratamiento de riesgos se establecen controles, procedimientos o mecanismos que disminuyen el impacto o la probabilidad de ocurrencia del incidente, se determina el impacto y se identifican áreas o procesos que deben implementar controles [9] . Las organizaciones deben ser conscientes que es imposible eliminar completamente el riesgo y que siempre quedará algo residual.

El análisis de riesgo debe cubrir todos los requerimientos de seguridad de la organización y las expectativas de las partes interesadas, es decir, en la elaboración del mapa de riesgos deben participar los representantes de cada área

[9]INTECO S.A. SGSI en una organización. [En línea]
<http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/>[Consultado 8 de Septiembre de 2013]

y estos a su vez deben haber consolidado previamente con su equipo de trabajo y con una metodología definida previamente, un barrido completo de sus actividades y procesos identificando y clasificando así los de impacto relevante como también aquellos que se van a asumir y mantener en niveles aceptables. De igual forma se deben tener en cuenta los recursos económicos, técnicos y humanos con los que cuenta ya que las inversiones deben ser proporcionales al valor de la información que se protege[10].

Este proceso apoya la toma de decisiones y plan de acción ante desastres y continuidad del negocio y además permite conocer el impacto económico, legal y operativo ante una falla de seguridad; debe estar detalladamente documentado de tal forma que haya resultados que comparar a medida que avanza el SGSI para conseguir los niveles de seguridad esperados.

El análisis de riesgos se basa en el inventario de activos. Estos se pueden clasificar según varias metodologías de análisis y gestión de riesgos, algunas de ellas son ISO/IEC 27005 o MAGERIT. MAGERIT fue elaborada por el Consejo Superior de Administración Electrónica de España, acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas"[11], los clasifica en 10 grupos:

- Servicios. Procesos de negocio ofrecidos al exterior o interior.
- Datos e información.
- Aplicaciones de software.
- Equipos informáticos.
- Personal. Incluye personal interno, subcontratado, clientes, etc.
- Redes de comunicaciones. Redes propias o subcontratadas de soporte para transmitir información.
- Soportes de información. Soportes físicos que permiten almacenar la información durante largos periodos de tiempo.
- Equipos auxiliares. Soporte a los sistemas de información que no están incluidos en otros grupos, por ejemplo teléfonos, fax, impresoras, cortadoras de papel, aire acondicionado, instalaciones.
- Edificios donde se alojan los sistemas de información, oficinas, vehículos.
- Intangibles. Imagen o reputación de la empresa.

[10] Modelo PHVA. Norma Técnica Colombiana NTC-ISO-IEC 27001
[11] INTECO S.A. SGSI en una organización. [En línea]
<http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/>[Consultado 8 de Septiembre de 2013]

Lo anterior indica que se debe realizar un inventario que identifique y clasifique los activos de información como también los riesgos asociados a estos, obteniendo así su descripción, ubicación y dueño. Cada área de la organización es quien conoce muy bien sus activos por lo tanto deben ser quienes definan el nivel de seguridad requerido para este. El enfoque de procesos toma entradas y produce resultados como salidas, esto quiere decir que los activos también se relacionan entre sí estableciendo dependencias. La idea es dibujar un árbol de dependencias que permita encontrar los procesos afectados por la materialización del riesgo en uno o varios de ellos. Este inventario facilitará la valoración de los activos con más importancia en el negocio y del impacto que un ataque sobre éste ocasione a la organización.

La implementación de un SGSI basado en la familia de normas ISO/IEC 27000 permite a la organización el ordenamiento de sus procesos y por lo tanto se logra identificar más fácilmente cuáles son las actividades críticas y que pueden generar mayor impacto en caso de materialización de un riesgo.

Se supone un éxito del SGSI cuando se involucra toda la organización liderada por la alta dirección debido a que es la que conoce la naturaleza del negocio, las tendencias en el mercado, fortalezas y debilidades y a su recurso humano, además es quien tiene el poder de inyectar cambios culturales y directrices necesarias para el buen funcionamiento del sistema, por lo tanto debe ser involucrado todo el organigrama operacional. También contribuyen al éxito, la conciencia de todo el personal por la seguridad de la información, que haya lideres frente al tema y que las responsabilidades no sean compartidas o globales, involucrar a los agentes externos y fortalecer valores sociales.

Los beneficios que una organización espera al implantar un SGSI son minimizar los riesgos hasta un nivel asumible, uso racional de los recursos, ahorros en inversiones por recuperación de desastres, cumplimiento de leyes que la protegen a sí misma como a sus clientes y proveedores y contar con un ciclo de vida ***Planear-Hacer-Verificar-Actuar*** para el manejo de la seguridad. También se obtiene una diferenciación en el mercado logrando mayor competitividad y finalmente el cumplimiento de objetivos.

Este proyecto permitirá ahorrar parte de los costos sobre consultorías para implementar un SGSI en la organización dado que se busca modelar procesos para gestionar el riesgo y los controles necesarios basados en los requisitos establecidos por la familia de normas técnicas ISO/IEC 27000.

Haciendo un análisis cualitativo, el impacto económico para cualquier organización es alto, es decir, aplicando una metodología de gestión del riesgo y selección de controles, las compañías tendrán un ahorro de costos por el uso racional de recursos en su implementación y ofrecerá el equilibrio entre los costos de los controles y su efectividad. No habrá inversiones innecesarias.

La protección de todos los activos de información identificados en el proceso es otro beneficio que garantiza la operación y, por lo tanto, la inversión y sus ingresos, así como también contribuye a la continuidad del negocio.

Por otro lado se cumplirá el aspecto legal. Las organizaciones disminuirán la probabilidad de verse involucradas en investigaciones, reclamaciones, demandas o indemnizaciones por parte de sus clientes y/o proveedores ya que por ejemplo, se respetarán sus derechos tratando un riesgo como divulgación de información no autorizada, aunque tal vez sea no intencionada.

Apuntando hacia un SGSI, las organizaciones mejorarán la competitividad y serán mejor calificadas por sus clientes y/o proveedores ya que serán más confiables y proyectarán una imagen sólida y segura.

El proyecto será fuente para el cambio cultural en aspectos de seguridad de la información ya que posiblemente influencie la población de interés para transformar la seguridad en una actividad de gestión, incluso podría ser útil para aplicarlos en la vida particular de las personas.

Dada la poca penetración de este tipo de sistemas en las organizaciones de la región, este proyecto se puede convertir en un buen punto de partida para nuevas investigaciones tanto académicas como empresariales relacionadas con la gestión de riesgos, lo que se traduce en un aporte investigativo importante, acortando el camino hacia la implementación y conocimiento de los SGSI en la región.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

- Modelar los procesos para gestionar el riesgo y seleccionar controles en la implementación del sistema de gestión de seguridad de la información en las organizaciones.

4.2 OBJETIVOS ESPECÍFICOS

- Establecer una guía de identificación y evaluación para el tratamiento de los riesgos.

- Establecer una guía para seleccionar los objetivos de control y los controles, así como el proceso a seguir para su aprobación dentro de la organización.

- Establecer una guía que permita medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

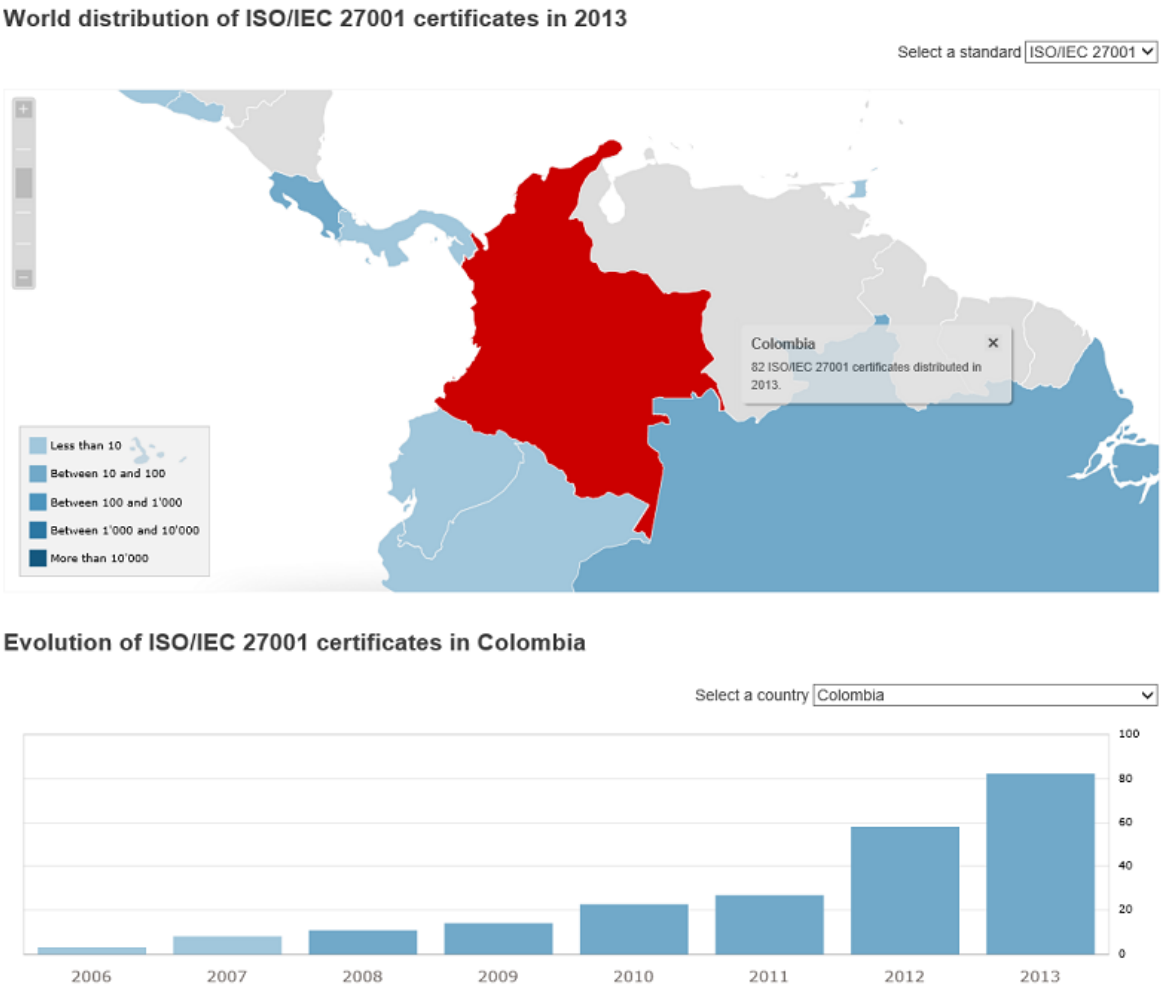
- Diseñar un proceso que facilite la revisión y valoración de los riesgos a intervalos planificados y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en la empresa, asegurando que el alcance siga siendo suficiente y que se identifiquen mejoras al sistema de gestión de seguridad de la información.

5. MARCO REFERENCIAL

5.1 MARCO DE ANTECEDENTES

Según la Organización Internacional de Estandarización – ISO, en Colombia hay 82 compañías certificadas en ISO/IEC 27001.

Figura 6: Número de empresas certificadas actualmente ISO/IEC 27001 en Colombia.[12]



[12]International Organization Standardization. [En línea] <http://www.iso.org/iso/home/standards/certification/home/standards/certification/iso-survey.htm> [Consultado 27 de junio de 2014]

Igualmente, se puede comparar el comportamiento de Colombia frente a otros países según este número de certificaciones obtenidas, notándose que a nivel suramericano Colombia ha mostrado un adelanto importante en la aplicación de la norma, estando al nivel de Brasil y por encima de países como Argentina y Chile, confirmando así mismo que las grandes economías mundiales apuestan seriamente por la obtención de este tipo de certificaciones, encontrando así los números que se muestran en la tabla número 1.

Cuadro 1: Relación de países certificados en ISO/IEC 27001[13].

Número de Certificaciones obtenidas en ISO/IEC 27001 a 2013	
País	Total
Japón	7084
India	1931
Reino Unido	1923
China	1710
USA	566
Colombia	82
Brasil	82
Argentina	40
Chile	24

La Compañía UNE EPM Telecomunicaciones es la primera Organización en Colombia y sexta en América Latina en certificarse en ISO/IEC 27001:2005 el 19 de Octubre de 2009.[14]

En la región, algunas organizaciones son conscientes de la necesidad del modelo, sin embargo no es posible determinar con exactitud el número de empresas certificadas en ISO/IEC 27001 en Risaralda por cuanto es difícil encontrar información en entidades certificadoras como ICONTEC la cual no ofrece esta información a través de su página web, así como tampoco el Registro Internacional de organizaciones certificadas en ISO 27001 a nivel mundial al que

[13] International Organization Standardization. [En línea] <http://www.iso.org/iso/home/standards/certification/home/standards/certification/iso-survey.htm> [Consultado 27 de junio de 2014]

[14] UNE Telecomunicaciones. [En línea] <http://www.une.com.co/nuestracompania/index.php?option=com_content&task=view&id=444> [Consultado 17 de Septiembre de 2013]

se accede por la página web www.iso27001certificates.com, ya que se encuentra fuera de servicio.

Como se observa en la figura 6, la adopción del estándar ISO/IEC 27001 en el país está apenas en desarrollo y como lo menciona el Ingeniero José Albeiro Rodríguez Patiño, en la entrevista citada en el capítulo 2, son las grandes organizaciones quienes tienen la iniciativa pero eso no indica que las pequeñas y medianas empresas no lo puedan implementar. También es notable que la mayoría de organizaciones propias de la región que adelantan el modelo de un SGSI, son sucursales de una sede central y a aquellas de origen netamente local no se les nota esta iniciativa**.**

5.2 MARCO TEÓRICO

La norma técnica ISO/IEC 27000 está enfocada en procesos, toda la organización se ve involucrada en su implementación en lo que a cada una le corresponde de tal manera que la suma de cada uno de los esfuerzos individuales, apoyados por la gestión y dirección de las personas que lideran el proceso, termine formando un SGSI que logre ejecutar todas las actividades de administración de riesgos incluyendo la creación de medidas ante tales riesgos y los controles para evaluar la efectividad de tales medidas.

La BSI (British Standards Institution) desde 1901 ha sido la primera organización de certificación a nivel mundial, ha publicado normas como:[15]

- BS 5750, año 1979 - ahora ISO 9001.
- BS 7750, año 1992 - ahora ISO 14001.
- BS 8800, año 1996 - ahora OHSAS 18001.

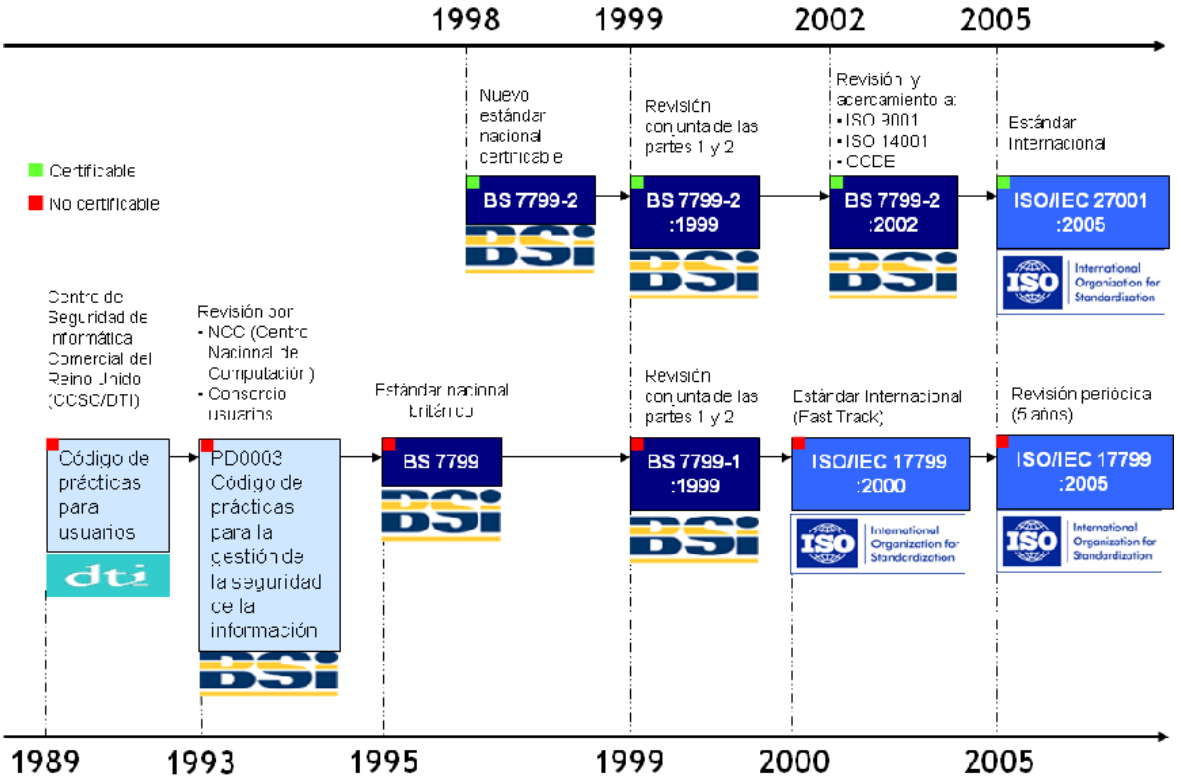
La norma BS7799 se publicó en 1995 con el fin de recomendar buenas prácticas para la gestión de la seguridad de la información. Esta fue adoptada por ISO en el año 2000, como ISO 17799.

[15] ISO 27000 en Español, [En línea] <http://www.iso27000.es/download/doc_iso27000_all.pdf> [Consultado 15 de Septiembre de 2013]

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007 manteniendo el contenido así como el año de publicación formal de la revisión. En Marzo de 2006, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información[16].

La figura 7 muestra cómo ha evolucionado a través de la historia el conjunto de códigos de mejores prácticas para usuarios de los sistemas de información, que nacieron en el Centro de Seguridad de Informática Comercial del Reino Unido en 1989, pasando por diferentes organizaciones internacionales que fueron puliendo tales códigos hasta convertirlos en lo que hoy se denomina Estándar Internacional ISO/IEC 27000.

Figura 7: Historia de ISO 27001 e ISO 17799.[17]



[16] ISO 27000 en Español, [En línea] <http://www.iso27000.es/download/doc_iso27000_all.pdf>p. 3. [Consultado 15 de Septiembre de 2013]
[17] LÓPEZ Neira, Agustín -RUIZSpohr, Javier. [En línea] <www.iso27000.es/download/HistoriaISO27001.pps> [Consultado 15 de Septiembre de 2013]

La familia de normas ISO/IEC 27000 son de aplicación voluntaria pero su uso a nivel mundial facilita las relaciones comerciales entre compañías internacionales y aumenta la competitividad en el mercado, también ayuda a mejorar la calidad y productos ofrecidos ya que este estándar internacional provee un modelo para establecer, implementar, operar y mantener un SGSI basado en los objetivos de la compañía, requisitos, requerimientos y expectativas de seguridad independiente del tamaño, estructura y razón de ser del negocio[18]. El modelo incorpora las mejores prácticas y recomendaciones de expertos que conforman el comité ISO/IEC JTC 1 SC 27 y que han reunido sobre el tema a nivel mundial[19].

ISO/IEC 27000 contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión[20].

ISO/IEC 27001 es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005.

ISO/IEC 27002 es desde el 1 de Julio de 2007, el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición y actualmente está en revisión la versión 2013. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios en la versión 2005 vigente y 14 dominios, 35 objetivos de control y 111 controles en la versión 2013 en revisión. A pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

ISO/IEC 27003, Publicada el 1 de febrero del 2010. Es una guía de implementación de SGSI e información acerca del uso del modelo PHVA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma

[18]INTECO S.A. SGSI en una organización. [En línea]
<http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/> [Consultado 14 de Septiembre de 2013]
[19] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO/IEC 27000 2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary.2009.
[20]INTECO S.A. SGSI en una organización. [En línea]
<http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/> [Consultado 14 de Septiembre de 2013]

BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO/IEC 27004. Publicada el 7 de diciembre del 2009. Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase Hacer del ciclo PHVA.

ISO/IEC 27005. Publicada en junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en las normas ISO/IEC 27001 e ISO/IEC 27002, es importante para un completo entendimiento de la norma ISO/IEC 27005:2008 que es aplicable a todo tipo de organizaciones.

ISO/IEC 27006. Es una guía para auditar al SGSI. Se encuentra en preparación. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información[21].

ISO/IEC 27007 Consiste en una guía de auditoría de un SGSI.

ISO/IEC 27799: Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias de salud[22].

De igual manera se adelantan normas para sectores específicos:

- ISO/IEC 27011, requisitos para telecomunicaciones elaboradas conjuntamente con la ITU (Unión Internacional de Telecomunicaciones)[23].
- ISO/IEC 27012 requisitos para la industria automotriz.

[21] ISO 27000 en Español, [En línea] <http://www.iso27000.es/download/doc_iso27000_all.pdf>p. 5. [Consultado 15 de Septiembre de 2012]
[22] Ibíd., p. 5.
[23] Ibíd., p. 5.

- ISO/IEC 27013 requisitos para la asociación mundial de loterías.
- ISO/IEC 27014 requisitos para sistemas de información en los transportes.
- ISO/IEC 27031 es una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
- ISO/IEC 27032 una guía relativa a la ciber-seguridad.
- ISO/IEC 27033 Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante Gateway, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y re numeración de ISO 18028.
- ISO/IEC 27034. Es una guía de seguridad en aplicaciones.

5.3 MARCO CONCEPTUAL[24]

- **Aceptación del riesgo:** Decisión de asumir un riesgo.

- **Activo:** Cualquier cosa que tiene valor para la organización.

- **Análisis de riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Disponibilidad:** Propiedad que define que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

[24] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO/IEC 27000 2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2009.

- **Evento de seguridad de la información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

- **Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.

- **Riesgo residual:** nivel restante de riesgo después del tratamiento del riesgo.

- **Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de reportar (*accountability*), no repudio y fiabilidad.

- **Sistema de gestión de la seguridad de la información: SGSI** parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

- **Tratamiento del riesgo:** proceso de selección e implementación de medidas para modificar el riesgo.

- **Valoración del riesgo:** proceso global de análisis y evaluación del riesgo.

5.4 MARCO LEGAL

Hoy día son cada vez más frecuentes las transacciones que se realizan por medios electrónicos, pago de servicios públicos, obligaciones financieras, etc. La educación es apoyada con plataformas tecnológicas que exigen interacción a través de internet. De igual forma el sector corporativo ha extendido sus operaciones gracias a la interconexión al mundo a través de internet. El mercado es cada vez más competitivo y los riesgos expuestos anteriormente son cada vez mayores y complejos.

Estos riesgos, entre muchos más, incluyen robos electrónicos, suplantación de identidades (phishing), piratería, sabotaje, malware, etc. El país no es ajeno a esta realidad, por tal motivo el Ministerio de Defensa Nacional por medio de la resolución 2057 del 15 de junio de 2007 definió que la dirección de Investigación Criminal de la Policía Nacional tratará la investigación de los temas de ciber seguridad y ciber defensa a través del Grupo Investigativo de Delitos informáticos con el fin de prevenir y atender este tipo de casos. El grupo mantiene comunicación con agencias internacionales para desarrollar los procesos judiciales y desactivar las páginas o grupos que generan algún tipo de amenaza. Como apoyo a esta tarea, la Policía Nacional ha dispuesto del Centro Cibernético Policial para la atención de denuncias de delitos relacionados con la ciber seguridad.

Por otro lado, antes del año 2009 no había una ley que castigara los delitos informáticos, se contaba con la Constitución Política Colombiana en el artículo 15 donde se promueve la intimidad personal y familiar, la Ley Estatutaria 1266 del 31 de Diciembre de 2008 que regula la información contenida en las bases de datos[25], la circular 052 expedida por la Súper Intendencia Financiera que dicta requerimientos mínimos de seguridad para el manejo de información a las entidades que vigila[26], la ley 527 del 18 de Agosto de 1999 donde se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales[27].

[25] LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008, [Documento En línea] <http://www.habeasdata.org.co/wp-content/uploads/2009/01/ley-estatutaria-1266-del-31-de-diciembre-de-2008.pdf> [Consultado 21 de Septiembre de 2012]

[26] Superintendencia Financiera de Colombia. Boletín 76 de 26/10/2007.[En línea] <http://www.superfinanciera.gov.co/NormativaFinanciera/Paginas/bolfinanciera2007_10.htm> [Consultado 21 de Septiembre de 2013]

[27] LEY 527 DE 1999, [Documento En línea] <http://www.secretariasenado.gov.co/senado/basedoc/ley/1999/ley_0527_1999.html> [Consultado 21 de Septiembre de 2013]

El 5 de Enero de 2009 el Congreso de la república aprobó la Ley 1273 "*Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelable – denominado 'De la Protección de la Información y de los Datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones".*

La Ley 1273 cobija el acceso abusivo y obstaculizar un sistema informático, interceptar datos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web, entre otras y considera situaciones de mayor punibilidad.

Aunque hay una pobre colaboración internacional, existen esfuerzos que despiertan la inquietud de la sociedad de la información, tal es el caso de la cumbre mundial realizada sobre el tema en Ginebra 2003 – Túnez 2005 donde se resalta el llamado a la confianza en la utilización de las TIC como se indica en la resolución 57/239 de la Asamblea General de las Naciones Unidas mediante conciencia y colaboración internacional. Por otro lado se destaca la importancia de enjuiciar la ciber-delincuencia donde se insta a los gobiernos a que promuevan leyes que lo hagan posible respetando los marcos vigentes, como por ejemplo las resoluciones de la Asamblea General de las Naciones Unidas 55/63 y 56/121 sobre la "Lucha contra la utilización de la tecnología de la información con fines delictivos" y el Convenio sobre el Delito Cibernético del Consejo de Europa[28].

[28] Cumbre Mundial sobre la Sociedad de la Información. Documento: WSIS-05/TUNIS/DOC/6(Rev. 1)-S [En línea] <http://www.itu.int/wsis/docs2/tunis/off/6rev1-es.html>> [Consultado 24 de Septiembre de 2013]

6. DISEÑO METODOLÓGICO

6.1 HIPÓTESIS

¿Será posible definir guías de procesos para el tratamiento de los riesgos, establecimiento de objetivos de control y controles que permitan medir su eficacia, según los requisitos definidos en la norma ISO 27001, y que puedan ser utilizadas por cualquier organización?

6.2 TIPO DE INVESTIGACIÓN

La investigación utiliza un método deductivo y analítico y se clasifica como de tipo descriptiva y explicativa.

6.3 METODOLOGÍA

Inicialmente, se realizará un completo estudio y análisis del grupo de normas ISO/IEC 27000.

Para modelar procesos se utilizarán herramientas informáticas como Bizzagi, la cual es un software para administrar procesos de negocios.

Por otro lado, se complementará y ajustará información a los procesos mediante la implementación de un escenario piloto en una organización de la región buscando así aplicarlo en condiciones reales del mercado.

Para tratar la gestión del riesgo se aplicará la metodología ISO/IEC 27005 y para seleccionar e implementar los controles buscando garantizar la reducción de estos hasta un nivel aceptable se aplicará la ISO/IEC 27002, teniendo en cuenta que es posible incorporar directrices adicionales propias relacionándolas a los numerales de la norma de tal forma que sean validados por las entidades certificadoras.

Se buscará apoyo con expertos en SGSI de la región o temas afines en normas ISO.

6.4 POBLACIÓN

El proyecto está dirigido inicialmente a una empresa de la región mediante una prueba piloto donde se busca validar que la implementación de las guías propuestas en este proyecto permitan implantar el SGSI en la organización. De igual manera está enfocado en general al sector empresarial de la región sin importar su actividad económica y que mediante la simulación pueda anticipar y mejorar sus procesos encaminándose desde un principio hacia una consultoría y/o auditoría.

De igual forma, la investigación es de interés para la población universitaria de pregrado y posgrado, para quienes deseen estudiar el grupo de normas y para quienes desarrollen proyectos relacionados.

7. PROCESO DE DISEÑO Y CONSTRUCCIÓN DE LA GUÍA

A continuación se describe el proceso mediante el cual se diseñó y construyó la guía propuesta para gestionar el riesgo.

7.1 CONSTRUCCIÓN DE LA GUÍA.

7.1.1. Consideraciones previas.

Para llevar a cabo el proceso de construcción de la guía, en primer lugar se definieron los parámetros a cumplir. Dado que las normas sobre gestión del riesgo están orientadas al cumplimiento de requisitos y recomendaciones generales y no son una metodología detallada que indique cómo hacer las actividades propias, se inició definiendo una hipótesis a comprobar buscando que una guía estructurada sirviera de interpretación de las normas y permitiera una gestión integral del riesgo para cualquier tipo de organización. Luego se planteó que tal guía se basara en una metodología estandarizada internacionalmente, por ello se estableció como soporte la familia de normas ISO/IEC 27000 pero incorporando recomendaciones de otras igualmente normalizadas.

Se estableció que la investigación sobre el tema utilizara un método deductivo y analítico con narración de tipo descriptiva y explicativa soportada además con el aporte de expertos en la materia y la experiencia de los autores.

También se concibió que la guía no sólo ofreciera una metodología para tratar el riesgo sino que enfocara los procesos bajo un Sistema de Gestión de Seguridad de la Información (SGSI) como herramienta de gestión integral para los activos de información y así mantener los principios de Confidencialidad, Integridad y Disponibilidad. Se pensó la guía para cumplir los requisitos de ISO/IEC 27001 y abrir el camino hacia una certificación en seguridad de la información. Fue así como se trazaron los objetivos para identificar, evaluar y tratar los riesgos como también seleccionar los objetivos de control y los controles dando insumos para medir su eficacia en el cumplimiento de requisitos de seguridad.

La metodología fue pensada para exigir en todo momento el compromiso de la alta dirección para tomar decisiones y aprobar resultados. Se asignan funciones y responsabilidades a esta y al grupo que lidera la tarea de gestión de riesgos, buscando la participación de todas las áreas del mapa de procesos incluidos en la gestión.

Se trazó la idea que debía ofrecer al mercado de la región, una herramienta de aplicación práctica para interpretar claramente en las normas ISO/IEC 27000 y apoyar la fase Planear en la implementación de un SGSI, incorporando de forma fácil e inmediata, aspectos particulares de las actividades propias de cada organización en la gestión del riesgo. Este método para gestionar el riesgo incluye el cumplimiento de aspectos legales para protegerse a sí mismo como también a clientes, proveedores y terceras partes.

Para la fase de diseño y construcción de la guía se inició con un estudio del problema a nivel mundial sobre los riesgos que se presentan para los activos de información y se enfocó progresivamente hacia el país y la región en cuya instancia además se estableció que gran parte de las empresas locales no cuentan con modelos de los procesos para hacer gestión de riesgos.

Se investigaron las amenazas desde las más simples como el código malicioso, pasando por ingeniería social y llegando incluso hasta cibercrimen y ciberterrorismo, abordando el impacto negativo hacia los resultados del negocio en términos económicos pero también cuantitativos en aspectos de imagen, legales, etc. Se evidenció en los estudios realizados que es relativamente fácil para una persona realizar ataques informáticos a datos confidenciales de una organización gracias a los avances tecnológicos y la facilidad de uso y disponibilidad en el mercado de estas herramientas. Cada vez los atacantes requieren menos conocimiento en el tema.

Se encontró que las amenazas son innumerables. Las relacionadas con temas informáticos cada año son más pero sin cambios sustanciales, con una tendencia a fraudes con fines económicos mediante software malicioso, ingeniería social y apoderamiento de equipos de forma remota para procesar información con fines delictivos. Se destaca también el empeño de los atacantes en encontrar las vulnerabilidades a aplicativos, sistemas operativos y protocolos de comunicaciones que permitan efectuar los ataques.

Por otro lado, se detectó que amenazas de otras categorías cobran mucha importancia y pueden materializar riesgos como inundaciones, cortes energéticos, incendios, indisponibilidad de comunicaciones, etc. Debido a lo anterior, la guía hace un énfasis en la valoración del riesgo, especialmente en la metodología de identificación de activos haciendo un amplio y detallado análisis en su clasificación e identificando sus responsables para obtener una valoración cuantitativa y cualitativa adecuada. Esta valoración es aprobada en segunda instancia por el dueño del proceso y el grupo SGSI Gestión del riesgo y avalada finalmente por la alta dirección.

Junto con el análisis de estadísticas históricas sobre eventos o incidentes de seguridad ocurridos sobre los activos de información, la guía facilita la identificación y valoración de amenazas y vulnerabilidades dando fuentes para ubicarlas y actualizarlas y por lo tanto permitiendo valorar los escenarios incidentes dada su combinación.

Se realizó un completo estudio y análisis del grupo de normas ISO/IEC 27000 y se buscó un marco genérico, metódico y detallado que permita el cumplimiento de requisitos y recomendaciones. De ISO/IEC 27000 se toma el marco teórico del SGSI y la descripción del ciclo PHVA y se alinean los conceptos a los términos y definiciones que incorpora. Cada actividad de la guía aporta al cumplimiento de los requisitos definidos en ISO/IEC 27001 para establecer, implementar, operar y monitorear el SGSI incluyendo documentos y registros mínimos que debe contener para evidenciar el grado de funcionamiento del sistema.

7.1.2. Construcción de etapas del proceso de gestión del riesgo.

Mediante el diagnóstico inicial del SGSI en la organización, la guía establece la forma de analizar el cumplimiento de la fase Planear de la norma frente a lo implementado, esto es fundamental para establecer los criterios de gestión del riesgo. También se orienta a modelar los procesos de tratamiento de riesgos y selección de controles tratados en el capítulo SGSI, en las secciones de Requisitos Generales, Establecimiento y Gestión, Implementación y Operación, Seguimiento y Revisión y Mantenimiento y Mejora del SGSI. La elaboración del contexto se apoya también en el proceso de gestión del riesgo e incorpora los criterios para seleccionar los objetivos de control y controles los cuales hacen parte del numeral 4.2.1 del estándar.

La metodología para gestionar el riesgo se soporta en ISO/IEC 27005 donde se conserva el ciclo PHVA desde la definición de criterios en el contexto, incluyendo los niveles para tomar decisiones en el flujograma de actividades hasta la actualización de resultados a todas las partes interesadas; y el monitoreo y revisión constante de niveles del riesgo. La metodología es cíclica con decisorios y conexiones entre fases que permiten redefinirse según los criterios definidos en el contexto. Consecuente con esto, se toman las recomendaciones de ISO/IEC 27002 para escoger objetivos de control y controles dando un orden específico de prioridad y cruce de factor común en su selección para racionalizar tiempo y costos facilitando las decisiones para el tratamiento de riesgos.

Para facilitar el manejo y compresión de la guía, se estableció una estructura agrupando actividades en cuatro etapas que corresponden a los objetivos del proyecto y al final en anexo al documento, una descripción detallada de cómo ejecutar cada actividad de tal forma que el usuario estará siempre ubicado y enfocado a lo largo del proceso. Cada actividad de la guía tiene tres componentes: Requisitos preliminares, Acción y Resultados. La Acción brinda instrucciones puntuales sobre cómo alcanzar el objetivo de la fase. Los Resultados sirven de insumo a la siguiente fase indicando cuáles se deben obtener y cómo documentarlos y almacenarlos.

La guía fue diseñada con un enfoque sistemático basado en procesos, incorporando mejora continua, iniciando con la planeación de criterios y actividades previas a la gestión del riesgo como tal. En este punto se incluye un diagnóstico inicial de la organización frente al sistema de seguridad de la información para determinar el grado de preparación que hay para implementarlo y también para ofrecer una visión de alto nivel de los recursos necesarios para tal fin, requiriendo un completo levantamiento de información. La guía continúa con la organización de la seguridad donde se crean los grupos que lideran el proceso de gestión del riesgo en la compañía y se asignan responsables y funciones. También se considera un plan de comunicación hacia toda la organización para crear cultura de seguridad y sensibilizarla sobre el tema.

La labor específica de gestionar el riesgo se alineó a ISO/IEC 27005 definiendo en el contexto el alcance y límites del mismo, detallando criterios para cada actividad e iniciando el primer ciclo del flujo en la ejecución de acciones. Entre ellos se analizan los procesos de la organización que harán parte de la gestión, se detallan los requisitos de seguridad de las partes interesadas y cómo realizar la valoración y tratamiento de riesgos. Lo anterior exige un conocimiento detallado a nivel de

misión, visión, políticas de calidad y seguridad, organigrama, mapa de procesos, activos de información, objetivos corporativos y planes estratégicos y marco legal aplicable a la compañía.

Luego de varios ejercicios sobre casos prácticos para estimar y evaluar el riesgo, se seleccionó el método conocido como ***Determinación del valor para la probabilidad y las consecuencias posibles de los riesgos*** descrito en ISO/IEC 27005. Con este se encontraron mejores resultados ya que combina la importancia de los activos y los efectos acumulativos de diferentes escenarios incidentes sobre el mismo activo, además permite realizar una análisis completo de la organización basado en sistemas (procesos o áreas de la compañía), priorizando fácilmente las acciones a seguir entre ellos y a su vez priorizar dentro de cada uno los activos a proteger.

Para la fase de tratamiento del riesgo se hizo necesario diseñar un esquema no tradicional mezclando los criterios de ISO/IEC 27002 y 27005 respectivamente, con un enfoque en racionalizar tiempo y recursos, empezando por los activos priorizados según la fase evaluación del riesgo y buscando seleccionar los objetivos de control y controles pertinentes en un orden específico según la criticidad de los dominios para la compañía. Posteriormente, se identificó en un factor común los controles necesarios nuevos, los existentes o particulares no listados en la norma para cumplir los objetivos planteados, luego filtrados por las restricciones que impliquen su uso; y por último, por el presupuesto aprobado para la inversión o actualización de controles.

Del anterior ejercicio resulta un registro clave para el proceso que se conoce como Declaración de Aplicabilidad, donde queda documentado tanto los objetivos de control y controles seleccionados como aquellos que no lo fueron, con la justificación debida y aprobado por la alta dirección. Cada control tendrá asignado un responsable quien definirá y documentará los indicadores de rendimiento sobre el activo protegido, validado por el grupo líder SGSI. También se encargará de realizar pruebas en un ambiente controlado, todo con el fin de activar las fases correspondientes del proceso de gestión.

Las opciones de tratamiento del riesgo van de lo más simple y práctico, pero no menos eficiente, que es retener y evitar, hasta acciones más complejas como reducir, transferir o como último esfuerzo una combinación de las anteriores. En toda instancia el nivel del riesgo es monitoreado para tomar decisiones según el flujograma de ISO/IEC 27005.

Debido a la experiencia y realimentación de expertos, se incorporó a la guía de manera opcional la elaboración del plan de continuidad de negocio como una alternativa de tratamiento a riesgos de muy alto impacto en términos desastrosos para al negocio, riesgos que no fueron considerados, no se pudieron evitar o que estuvieron muy por encima de niveles tolerables para la organización. Esto con el fin de garantizar el nivel de servicio en los límites definidos, racionalizando recursos y con el objetivo de recuperar completamente la operación.

Se ordenó la guía conforme a la Comunicación del riesgo mediante una comunicación permanente en cada fase del proceso del equipo de trabajo SGSI, dueños de procesos y áreas específicas para permitir una compresión continua, alinear planes, recibir realimentación desde todos los frentes de trabajo y compartir resultados. Así mismo ocurrió en la fase Monitoreo y revisión del riesgo. Oportunamente en cada actividad y no al final del proceso se producen insumos y se motivan acciones basadas en un amplio cambio de variables, canalizando sus resultados y decisiones en el grupo SGSI.

Por último, se vio necesario establecer un plan de comunicaciones que también recibe insumos de todas las fases del proceso. Aquí se crea una cultura corporativa de seguridad de la información y se notifican avances y resultados en la implementación del proceso de gestión del riesgo, haciendo uso de campañas internas vía carteleras, intranet, correo electrónico, agenda en comités de área, etc.

Se complementa y ajusta la guía mediante la implementación de un escenario piloto en una empresa de orden nacional que hace presencia en la región, buscando así aplicarlo en condiciones reales del mercado obteniendo resultados satisfactorios.

Finalmente, se diseñó una encuesta que fue publicada en la web mediante Google Drive para facilitar el acceso y se contactaron nueve (9) expertos de la región para que evaluaran la guía y recibir de ellos una realimentación sobre la metodología planteada. Los resultados de esta encuesta se exponen en el capítulo siguiente.

7.2 DIFICULTADES DURANTE LA CONSTRUCCIÓN.

Naturalmente fueron varias las dificultades presentadas para desarrollar la guía. La más representativa, fue que las normas ISO/IEC 27000 están orientadas al cumplimiento de requisitos y recomendaciones generales y no son una metodología detallada que indique cómo realizar las actividades específicas.

La diversidad de sectores empresariales en la región, cada uno con una buena cantidad de organizaciones las cuales a su vez tienen negocios específicos, tamaño variable y procesos particulares, hacen mayor la complejidad de diseñar una guía única para gestionar el riesgo. Por ello, fue útil la experiencia de los autores para enmarcar las actividades dentro de un proceso de gestión en una forma genérica y metódica, pero aún más detallada y especifica indicando cómo hacer las tareas que llevan al cumplimiento de requisitos y sugerencias indicadas por las normas.

Estructurar la guía fue una tarea compleja debido al gran volumen de información a tratar, generar y almacenar. Consolidar los datos obtenidos fue una labor simplificada mediante el uso de tablas dinámicas de la aplicación Excel del paquete Microsoft Office. Tener claro los objetivos del proyecto fue clave para alinear el formato a un método ordenado, continuo y consistente.

La seguridad de la información es un tema que en gran medida, en la población corporativa de la región, hasta ahora no tiene la acogida debida, especialmente enmarcado bajo un SGSI e incorporado a un Sistema de Calidad existente, generando así un Sistema Integrado de Gestión. Por lo tanto, este aspecto no facilita sensibilizar a las organizaciones para que pongan en práctica esta guía.

Por otro lado, las compañías de la región que sí tienen implementado o en desarrollo el SGSI, poseen políticas y directrices definidas, complicando la práctica de este proyecto, especialmente las de orden nacional cuyos encargados del tema están ubicados fuera del departamento de Risaralda. Se suma a esto la confidencialidad y delimitación de la información suministrada por las organizaciones que buscan siempre protegerse ante la filtración de información institucional.

Teniendo en cuenta las características de la prueba piloto, no fue posible desarrollarla en su totalidad debido a los conflictos que esto podría causar dentro de la organización sobre todo en la etapa de ejecución de actividades, ya que

estas podrían interferir con las propias programadas dentro de su Sistema Integrado de Gestión, cuando de informar a todos los colaboradores se trata. Otra limitante es la asignación de recursos para implementar controles durante la ejecución de una prueba piloto propiciada como un trabajo académico que no garantiza continuidad en la organización.

Por último, en la región no abundan los profesionales expertos en el tema que sirvan de apoyo en el desarrollo de la investigación y recibir realimentación de los resultados obtenidos en el producto final. Los profesionales consultados presentaban una alta ocupación en sus oficios y no disponían fácilmente de tiempo libre para dedicarlo al proyecto.

8. ANÁLISIS DE APLICABILIDAD DE LA GUÍA

8.1 EVALUACIÓN DE EXPERTOS

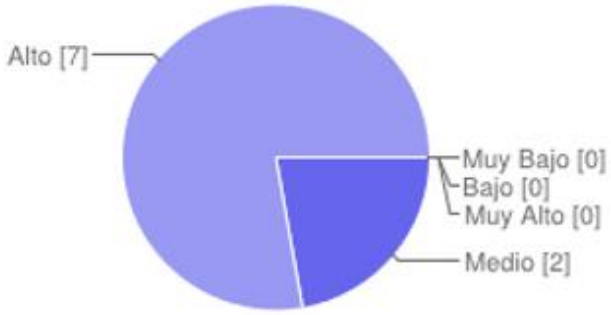
Las preguntas de la encuesta dispuesta para la evaluación de los expertos fueron diseñadas de tal forma que evidenciaran el grado de cumplimiento de las fases de la guía para gestionar el riesgo, que a la vez reflejan el de los objetivos del proyecto por estar alineados entre sí. Al final se solicitó evaluar en forma general si la aplicación de la guía permitiría gestionar el riesgo de forma exitosa en una organización de la zona, requiriendo además la justificación de la respuesta del experto. También a su juicio, se pidió cuantificar el grado de apoyo que ofrece la guía para implantar un SGSI.

Los expertos fueron seleccionados de acuerdo a su relación con el tema desde la academia y/o desde su experiencia laboral, buscando que su análisis sobre la guía fuera consistente con la realidad de la región.

Se muestran a continuación los resultados obtenidos:

Pregunta No. 1: ***¿En qué grado considera usted que la metodología planteada en la guía logra diagnosticar acertadamente la situación actual del SGSI en la compañía, como punto de partida para iniciar con el proceso de Gestión del Riesgo?***

Figura 8. Resultados de la pregunta No. 1 de la encuesta a expertos.

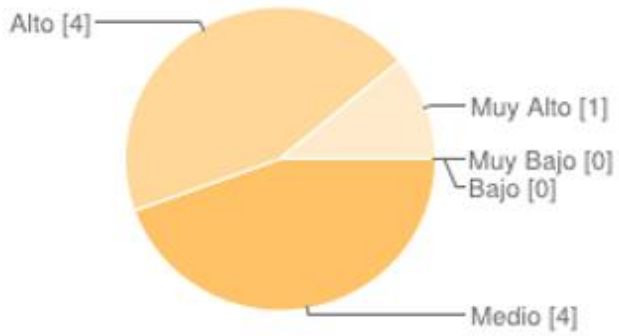


Muy Bajo	0	0%
Bajo	0	0%
Medio	2	22%
Alto	7	78%
Muy Alto	0	0%

En este aspecto, el 78% de los especialistas indican que se logra el objetivo en un alto grado. Esta valoración se considera consecuente con el diseño de la acción donde el levantamiento de información abarca todos los puntos requeridos por el estándar ISO/IEC 27001 en la fase Planear capítulos 4.2.1 Establecimiento y Gestión SGSI, 4.2.2 Implementación y Operación SGSI, 4.2.3 Seguimiento y Revisión SGSI y 4.2.4 Mantenimiento y Mejora SGSI.

Pregunta No. 2: ***¿En qué grado considera usted que la guía establece y explica claramente los pasos necesarios para cumplir con la etapa de análisis del riesgo (identificación + estimación) según los requerimientos de la norma ISO/IEC 27001?***

Figura 9. Resultados de la pregunta No. 2 de la encuesta a expertos.

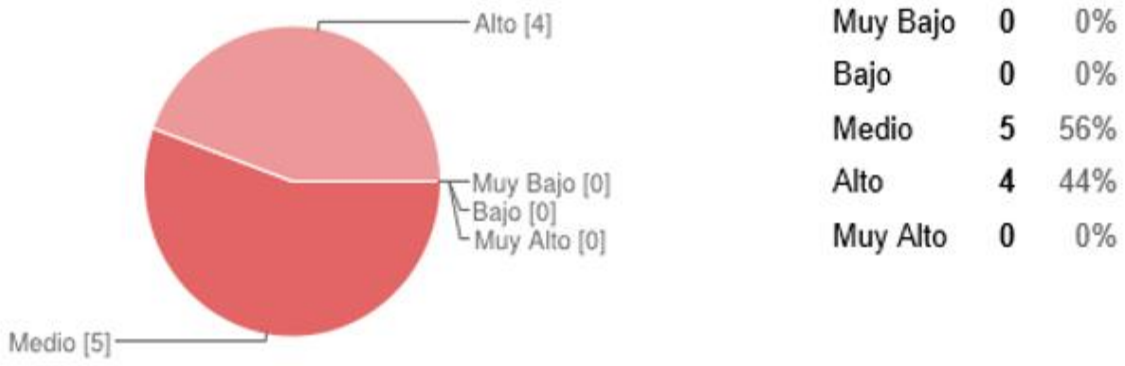


Muy Bajo	0	0%
Bajo	0	0%
Medio	4	44%
Alto	4	44%
Muy Alto	1	11%

El 55% de los expertos indican que se cubren los requisitos entre un nivel alto y muy alto. Se incluye este aspecto bajo las recomendaciones dadas en el capítulo 9 dado que se esperaba un mejor resultado considerando que hay aspectos de valor agregado frente a las metodologías típicas como la organización de la seguridad, definición de requisitos de seguridad, asignación de presupuesto, análisis de estadísticas históricas, identificación de controles existentes, filtros de resultados a cargo del comité SGSI y un método amplio y suficiente para estimar el riesgo que permite realizar un análisis completo de la organización basado en sistemas (procesos o áreas de la compañía), priorizando fácilmente las acciones a seguir entre ellos y a su vez priorizar dentro de cada uno los activos a proteger.

Pregunta No. 3: ***¿En qué grado considera usted que la guía plantea una metodología válida y efectiva para la evaluación de los riesgos?***

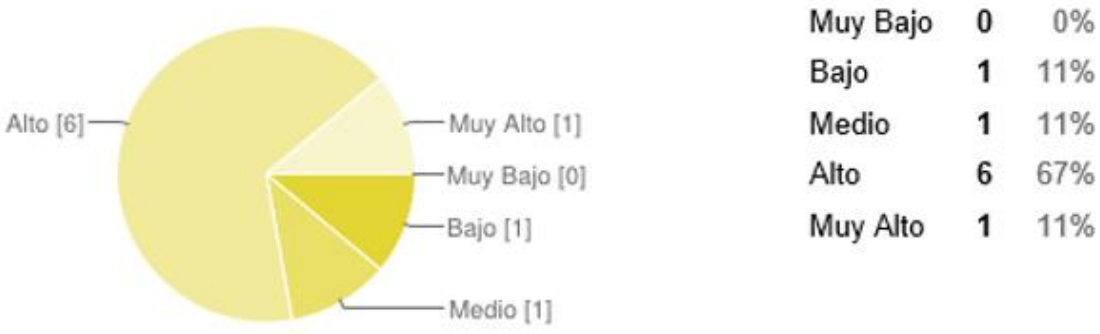
Figura 10. Resultados de la pregunta No. 3 de la encuesta a expertos.



Este aspecto también se remite a las recomendaciones dadas en el capítulo 9 ya que se proyectaba un concepto alto entre la mayoría de especialistas. Pese a contar con un método de análisis amplio e incluido en la norma ISO/IEC 27005 que trata la organización como la suma de sistemas individuales permitiendo priorizarlos entre sí y al asociarlos frente a indicadores operacionales, el concepto de cumplimiento está distribuido entre medio y alto con un 56% y un 44% respectivamente.

Pregunta No. 4: ***¿En qué grado considera usted que la guía plantea una metodología válida y efectiva para la selección de Objetivos de Control y Controles según los requerimientos de la compañía y ceñida a lo establecido en la norma ISO/IEC 27002?***

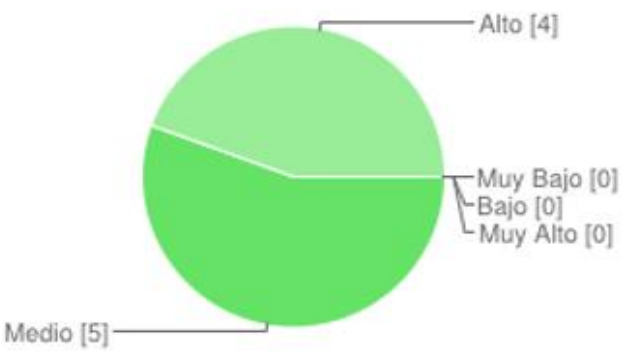
Figura 11. Resultados de la pregunta No. 4 de la encuesta a expertos.



En este aspecto, el 78% de los analistas ve un alto grado de validez y efectividad de la metodología. Motiva este resultado, el análisis que propone la guía en un orden definido para los dominios de seguridad y así tratar los más estratégicos en primer lugar, incluyendo luego de un filtro de factor común y restricciones, controles particulares nuevos o existentes que están o no especificados en la norma y asignándoles un responsable, permitiendo consolidar así de forma amplia la declaración de aplicabilidad y racionalizando recursos para que el tratamiento de riesgos sea eficiente.

Pregunta No 5. ***¿En qué grado considera usted que la guía plantea una metodología válida y efectiva para medir la eficacia de los controles seleccionados?***

Figura 12. Resultados de la pregunta No. 5 de la encuesta a expertos.

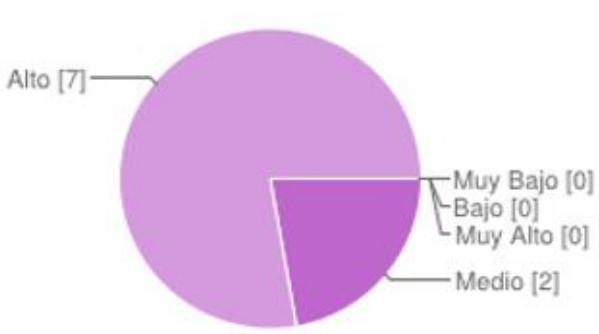


Muy Bajo	0	0%
Bajo	0	0%
Medio	5	56%
Alto	4	44%
Muy Alto	0	0%

El concepto recibido se ubica entre medio y alto con un 56% y un 44% respectivamente. Este es otro punto a incluir en las recomendaciones dadas en el capítulo 9 ya que se esperaba un concepto más alto debido a que hay aspectos que marcan la diferencia como por ejemplo: desde la fase tratamiento del riesgo cuando son seleccionados los controles, la guía considera un responsable idóneo para cada control encargándolo de definir indicadores, metas de cumplimiento y realizar pruebas simuladas de rendimiento en ambiente controlado y generar reportes y alertas como insumo a la fase monitoreo y revisión del riesgo.

Pregunta No. 6: ***¿En qué grado considera usted que la guía plantea una metodología válida y efectiva para hacer seguimiento, revisión y valoración periódica de los riesgos?***

Figura 13. Resultados de la pregunta No. 6 de la encuesta a expertos.

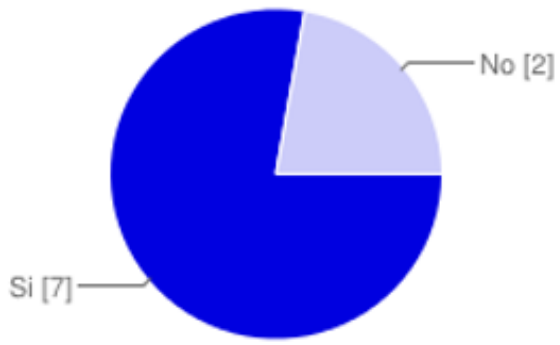


Muy Bajo	0	0%
Bajo	0	0%
Medio	2	22%
Alto	7	78%
Muy Alto	0	0%

El 78% de los expertos consideran un alto grado de cumplimiento para este caso. El diseño de la fase de monitoreo y revisión del riesgo consideró insumo desde las otras fases en todo momento para cumplir satisfactoria y oportunamente acciones preventivas y correctivas ante cualquier variable que dispare esta acción.

Pregunta No 7. ***¿En términos generales, considera usted que con la aplicación de esta guía en una empresa de la región, es posible gestionar los riesgos y seleccionar los controles como parte de la implementación de un Sistema de Gestión de Seguridad de la Información?***

Figura 14. Resultados de la pregunta No. 7 de la encuesta.



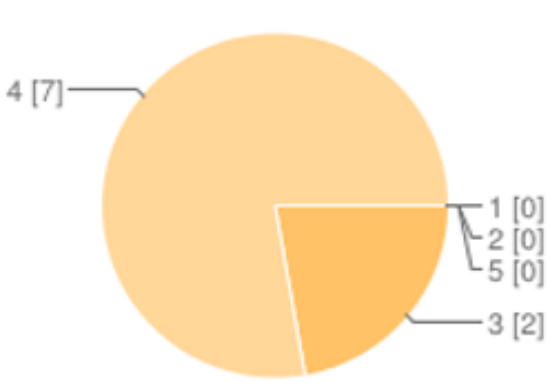
Si	7	78%
No	2	22%

Nuevamente el 78% de los analistas considera viable la aplicabilidad de la guía para gestionar el riesgo y dicho concepto está alineado con los resultados de la prueba piloto mostrados en el numeral 8.2. La pregunta pide que los expertos expliquen el *¿Por qué*? de su respuesta. Quienes aprueban la aplicabilidad de la guía coinciden en que esta conserva la esencia de las normas ISO/IEC 27000 orientando al usuario de forma clara, práctica y en fases ordenadas lógicamente según el estándar para realizar el proceso de gestión de riesgos.

Por otra parte, no es posible establecer un factor común entre los conceptos dados por parte de quienes respondieron negativamente esta pregunta pues estos indican que puede haber subjetividad en la asignación de valores a la probabilidad de ocurrencia de escenarios incidentes y falta de información para identificar y evaluar los riesgos, sugiriendo una metodología didáctica y que exponga ejemplos prácticos. Este aspecto será incluido en las recomendaciones del capítulo 9 para mejorar los resultados del proyecto.

Pregunta No. ***8: Según su experiencia, por favor Califique de 1 a 5 el valor que la utilización de esta guía podría agregar a los responsables de la implementación del SGSI en una empresa, donde 1 es un bajo valor agregado y 5 representa el mayor valor agregado.***

Figura 15. Resultados de la pregunta No 8 de la encuesta.



1	0	0%
2	0	0%
3	2	22%
4	7	78%
5	0	0%

Se mantiene la tendencia sobre la alta valoración referida al cumplimiento general de la guía para gestionar el riesgo, indicando el apoyo y complemento que esta representa para la implementación de un sistema de seguridad de la información en una compañía de la región, basados en el conocimiento y experiencia de quienes la evaluaron.

8.2 EVALUACIÓN DE LA PRUEBA PILOTO

Con el fin de validar la aplicabilidad de la guía en una empresa real, se realizó una prueba piloto en la cual se aplicarían una a una las actividades propuestas en ella y para eso se logró establecer contacto con una compañía de orden nacional con presencia en la región y que tiene en fase de implementación un SGSI. El desarrollo completo de la prueba piloto se encuentra documentado en el anexo B.

Cuando se expuso la propuesta para la aplicación de la prueba piloto ante la Dirección Regional y Grupo interesado de la Entidad, su aprobación fue rápida ya que fue considerada una buena oportunidad para detectar mejoras en sus procesos a nivel zonal. A pesar de contar con directrices centrales sobre el SGSI, la Dirección Regional cuenta con cierto grado de autonomía para ejecutar las actividades relacionadas. Fue así como se recibió licencia para trabajar sobre procedimientos estratégicos que demuestran gestión de la regional y cuya cobertura es amplia por el número de sedes y agentes externos involucrados.

Se contó con un alto grado de apoyo y compromiso por parte de la organización, facilitando los recursos técnicos y profesionales de cada área, llevando a cabo varias sesiones de trabajo para los análisis requeridos que implicaba una alta carga laboral para los funcionarios.

El diagnóstico inicial del estado del SGSI en la compañía, indicó un grado de avance del 53% en la implementación, referida solamente a la fase Planear respecto a lo indicado por la norma. Con la aplicación de la guía se cerró la brecha entre lo que había implementado y lo que se requiere para obtener la certificación pues se lograron cubrir todos los aspectos propuestos de la norma.

Pese a contar con un SGSI en implementación, la regional no contaba con responsables ni responsabilidades claras para actuar frente al proceso de gestión del riesgo en las actividades bajo su autonomía.

La fase de valoración y tratamiento de riesgos que se realizó bajo la aplicación de la guía, fue más amplia que la realizada bajo su sistema interno. Fue así como su identificación, estimación y evaluación permitió tratar las actividades en la zona con mayor profundidad y acorde a sus necesidades, facilitando identificar claramente el riesgo aceptable por la regional. Esto es entendible dado la cantidad de procesos y funcionarios a nivel nacional que tiene la entidad.

Esta aplicación práctica de la guía permitió hacer ajustes a su metodología debido a la identificación de casos particulares que impactaban aspectos generales. Igualmente, facilitó que la organización a nivel zonal ampliara su proceder en cuanto a seguridad de la información, identificando activos no previstos y utilizando todos los controles de los que ya disponían pero que no explotaban su potencial, es decir, hubo una trasferencia de experiencia y conocimiento entre las partes.

No fue posible ejecutar todas las fases de la guía. El grupo de Planeación de la organización que a su vez tenía el rol de comité de gestión SGSI en la prueba piloto, identificó un posible conflicto y dificultad si se implementaban las fases III Medición de eficacia de los controles y IV Seguimiento, revisión y valoración periódica de riesgos debido a las actividades propias del sistema integrado de gestión en servicio, la criticidad de los procesos, el número de sedes y agentes externos involucrados, la carga laboral de los funcionarios, el tiempo requerido para medir resultados y el mismo alcance de la guía. Sin embargo, el comité de gestión analizó la metodología y la consideró adecuada para cumplir el objetivo de las fases en otro escenario de prueba piloto.

9. CONCLUSIONES

La guía desarrollada no se limita a gestionar el riesgo, tiene un alcance mayor ya que trata el proceso bajo el esquema de un SGSI ofreciendo a sus usuarios un valor agregado importante.

El proceso de gestión requiere de una dedicación permanente y continua, exige compromiso de la alta dirección y recursos destinados a garantizar su planeación, implementación, actualización, monitoreo y revisión.

El método utilizado en la fase valoración del riesgo analiza los procesos de la organización como sistemas individuales permitiendo priorizarlos entre sí, midiendo el impacto acumulativo de todos los escenarios sobre un mismo activo.

La fase tratamiento de riesgos de la guía racionaliza recursos e inversiones, buscando que la organización maximice el uso de los controles existentes y se consideren en primer lugar formas sencillas pero efectivas para enfrentarlos.

La metodología incorpora acciones de mejora continua, comunica el riesgo en todas las instancias del proceso, reúne insumos oportunos para su monitoreo y revisión, como también divulga los planes y sensibiliza la organización hacia una cultura de seguridad de la información.

La evaluación de especialistas a este proyecto pronosticó un alto grado de éxito en su aplicación general para gestionar el riesgo en una empresa de la región y como apoyo para implantar un SGSI, un alto grado de cumplimiento frente a las normas ISO/IEC 27000. Dichas normas son globales, no detalladas y por ello algunos aspectos analizados por los evaluadores ante esta propuesta se agrupan por igual porcentaje entre bueno y muy bueno, razón por la cual se plantearon recomendaciones a los temas análisis, evaluación de riesgos y medición de eficacia de controles. Posiblemente la estructuración de la guía y su explicación detallada como documentos separados no facilitó la comprensión de criterios al momento de evaluarla.

La prueba piloto aplicada a una empresa de la región, demostró aplicabilidad de la guía para gestionar el riesgo, ofreció resultados satisfactorios demostrando que aunque una organización tenga un SGSI en construcción, es posible mejorarlo, ajustarlo y/o generar nuevos procedimientos al respecto.

10. RECOMENDACIONES

Es necesario para el usuario que durante la práctica cuente con el documento completo de la guía, su anexo sobre la descripción detallada de actividades en cada fase y las normas ISO/IEC 27000, ya que el volumen de información a administrar puede llegar a ser considerable en alguna instancia del proceso y maniobrar con un solo soporte puede inducir a confusión en los conceptos y desviar el curso de la metodología planteada. Puede facilitar esta labor compilar la guía y su anexo detallado como un solo documento.

Para futuras versiones del proyecto:

- Una actualización de la metodología por lo menos cada dos (2) años para ordenarlo conforme a las actualizaciones de las normas ISO/IEC 27000 y/o diferentes metodologías normalizadas, como también requisitos de las empresas de la región.

- Se propone hacer un contacto personalizado con los expertos acercados e involucrar nuevos participantes, compartir conceptos que permitan ampliar, aclarar temas y validar si es necesario ajustes en los aspectos que tuvieron calificación distribuida por igual media y alta en la valoración realizada, como lo fue el análisis y evaluación de riesgos y medición de eficacia de controles.

- Realizar pruebas pilotos periódicamente y que cubran todas las fases de la guía para confrontar la realidad del sector empresarial en la región.

- Para el grupo de investigación Nyquist de la Universidad Tecnológica de Pereira sería muy útil publicar en una página web el documento de la guía y habilitar un buzón de sugerencias para los usuarios que hayan experimentado con ella, de tal forma que se reciban retroalimentaciones y se incorporen mejoras dando continuidad al proyecto.

- Ampliar el alcance la guía para que se incorpore el SGSI a un Sistema de Calidad existente y generar un Sistema Integrado de Gestión.

- Realizar un desarrollo de software que facilite la gestión del riesgo a través de una interfaz gráfica amigable, que contenga un módulo de ejemplos prácticos y que almacene los diferentes registros y resultados del proceso.

BIBLIOGRAFÍA

ALLEN, Julia H. *Information Security as an Institutional Priority.* Disponible en: <http://www.cert.org/archive/pdf/info-sec-ip.pdf>

Ciberseguridad: Colombia ante un ataque. Disponible en: <*www.gerente.com/detarticulo.php?CodArticl=385*>

Cumbre Mundial sobre la Sociedad de la Información. *Documento: WSIS-05/TUNIS/DOC/6 (Rev. 1)-S.* Disponible en: <*http://www.itu.int/wsis/docs2/tunis/off/6rev1-es.html*>

IBM Report: Surge in CRIMINAL-DRIVEN CYBER ATTACKS Disponible en: <*https://www-03.ibm.com/press/us/en/pressrelease/19141.wss*>

ICONTEC. (2006). *Norma Técnica Colombiana NTC-ISO/IEC 27001 - Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.* Bogotá: ICONTEC.

ICONTEC. (2009). *NTC-ISO/IEC 27005 Norma Técnica Colombiana. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.* Bogotá: ICONTEC.

Informe anual de fraude Online y Cibercrimen 2012. Disponible en: <*http://www.s21sec.com/descargas/informe_anual_fraude_2009.pdf*>

INTECO S.A. (25 de Mayo de 2013). *SGSI en una organización.* Obtenido de http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2009). *ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Suiza.

ISO 27000 en Español. Disponible en :
<http://www.iso27000.es/download/doc_iso27000_all.pdf>

LEY 527 DE 1999, Disponible en:
<http://www.secretariasenado.gov.co/senado/basedoc/ley/1999/ley_0527_1999.html>

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008. Disponible en: *<http://www.habeasdata.org.co/wp-content/uploads/2009/01/ley-estatutaria-1266-del-31-de-diciembre-de-2008.pdf>*

LÓPEZ Neira, Agustín – RUIZ Spohr, Javier. Disponible en:
<www.iso27000.es/download/HistoriaISO27001.pps>

Revista América Económica, Política y Sociedad. Disponible en: *<http://www.americaeconomia.com/politica-sociedad/politica/colombia-advierte-sobre-riesgo-de-ataque-informatico-durante-elecciones>*

Superintendencia Financiera de Colombia. *Boletín 76 de 26/10/07.* Disponible en: *<http://www.superfinanciera.gov.co/NormativaFinanciera/Paginas/bolfinanciera2007_10.htm>*

UNE Telecomunicaciones. Disponible en:
<http://www.une.com.co/nuestracompania/index.php?option=com_content&task=view&id=444>

VILLA SÁNCHEZ, Paula A. *Definición de procesos de auditoría interna del sistema de gestión de seguridad de la información soportado en TIC.* Pereira (Rda). Universidad Tecnológica de Pereira, 2011.

ANEXO A
GUÍA PROPUESTA PARA LA GESTIÓN DEL RIESGO

El estándar ISO/IEC 27001 define un Sistema de Gestión de Seguridad de la Información (SGSI) basado en procesos bajo el modelo Planear-Hacer-Verificar-Actuar (PHVA) el cual se utiliza para operar y mantener el sistema. En cada fase se establecen las actividades a realizar con el fin de conformar el sistema dentro de una operación eficiente.

Cualquier organización busca como uno de sus objetivos principales, mantener su negocio en continua operación. Asegurar la información vital se hace necesario e indispensable. Una herramienta de gestión que permite esta labor es implementar un SGSI ya que disminuye los riesgos a los que se someten los activos de información.

Una de las actividades claves es conocer los procesos corporativos e identificar los activos de información, sus características y las dependencias que permiten obtener un producto o servicio propio del negocio, también se debe conocer sus amenazas y enfrentarlas adecuadamente. Así es más fácil organizar los sistemas de información, establecer políticas y/o procedimientos y definir controles que mediante la medición periódica de su eficacia disminuirán los eventos de seguridad. Cuándo existen controles para minimizar o evitar la ocurrencia de un riesgo y este se materializa, se denomina evento. Se llama incidente cuando las consecuencias del riesgo se sufren y no han sido previstas.

Es importante para la alta dirección de la organización y para quienes deben documentar y ejecutar los procesos de implementación del SGSI o solamente para realizar la fase de gestión del riesgo, iniciar con la fase planear definiendo un estado preliminar que indique qué tan preparada se encuentra la organización para afrontar la implantación del nuevo sistema y ayudar así a identificar los recursos que se requieren para comenzar con el proceso. Para esto se debe realizar un completo levantamiento de información que cubra cada uno de los temas exigidos por la norma ISO/IEC 27001 y que además cada punto sea medible tanto cualitativa como cuantitativamente, para que de esta manera se pueda definir cuáles son los procesos que exigen mayor atención de acuerdo a su

calificación y para llevar un control sobre el avance general de la implementación del alcance definido en el SGSI o para realizar la gestión del riesgo exclusivamente.

Los incidentes y eventos de seguridad son aquellas amenazas que explotan una vulnerabilidad de un activo de información materializándose en un riesgo. Por lo tanto gestionar el riesgo a través de un SGSI es un proceso cuyo objetivo es mantenerlos en un nivel aceptable para la organización amparando así la confidencialidad, integridad y disponibilidad de los activos de información ante clientes, proveedores, para sí mismo y cualquier parte interesada en el negocio; el resultado final es asegurar los objetivos de rentabilidad del oficio.

Los controles implementados reducirán los riesgos al nivel aceptable, si se producen daños serán de bajo impacto y la continuidad del negocio se asegura. Se deriva de esto un ahorro en los costos que implica prever y racionalizar recursos eliminando inversiones innecesarias o mal diseñadas generando ineficiencia, incumplimiento del marco legal y contractual. Finalmente la Seguridad pasa de ser una serie de actividades organizadas a tener un ciclo de gestión.

Para que el ciclo de gestión funcione adecuadamente, requiere el compromiso y liderazgo de la alta gerencia de la organización debido a su conocimiento y experiencia en el negocio y por su capacidad para implantar nuevos procedimientos en los procesos.

En las compañías donde se esté trabajando para implementar un Sistema Integral de Gestión o que ya se haya implantado por lo menos otro sistema de calidad, se deben ajustar procesos y/o procedimientos ya definidos en su marco operativo, logrando trabajar en paralelo las tareas que involucren todos los sistemas, para evitar reproceso y manteniendo la coherencia entre las actividades de cada sistema.

A.1. ESTRUCTURA DE LA GUÍA

La guía establece el cumplimiento de actividades enfocadas en cuatro etapas para gestionar el riesgo:

- Identificación y evaluación para el tratamiento de los riesgos.
- Selección de Objetivos de Control y controles.

- Medición de eficacia de los controles.
- Seguimiento: Revisión y Valoración periódica de riesgos.

Cada actividad de la guía establece unos pasos para su cumplimiento:

- Requisitos: Son los datos preliminares y necesarios para cumplir la actividad.
- Acción: Es el objetivo que se busca al desarrollar la actividad, describiendo la forma de realizarla.
- Resultados: Es la información obtenida luego de procesar los requisitos bajo la acción descrita.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

La guía se fundamenta en el conjunto de normas internacionales ISO/IEC 27000 que definen el marco de un Sistema de Seguridad de la Información para gestionar el riesgo. Estas normas han sido diseñadas por ISO, Organización Internacional de Normalización, y por IEC, Comisión Electrotécnica Internacional. Estas entidades son constituidas por los organismos de normalización formales de cada país. En el caso de Colombia es ICONTEC quien nombra las normas como PROYECTO DE NORMA TECNICA COLOMBIANA NTC-ISO/IEC 27000. Para tal fin ISO e IEC han establecido un comité técnico de trabajo llamado ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques[29].

A continuación se hace una descripción de cómo se alinea la guía con cada norma del grupo.

ISO/IEC 27000:2009 presenta un resumen de la familia de estándares, ofrece una introducción a un SGSI, describe el ciclo Planear-Hacer-Verificar-Actuar (PHVA) y

[29] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO/IEC 27000 2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2009.

presenta términos y definiciones usadas en las normas para precisar términos y evitar confusiones. La guía basa en ella, su fundamento teórico y conceptos.

El estándar ISO/IEC 27001 es universal para cualquier tipo de compañía, es certificable y auditable, especifica los requerimientos para establecer, implementar, operar, monitorear, y mantener un SGSI basado en procesos bajo el modelo PHVA. El alcance la presente guía es el cumplimiento de la fase Planear y la trata como un subsistema que contiene a su vez un ciclo PHVA, se introduce entonces los conceptos de sub ciclos *Planear-Planear, Planear-Hacer, Planear-Verificar y Planear-Actuar.* Esta norma establece en cada fase las actividades a realizar con el fin de conformar el sistema dentro de una operación eficiente. Incluye un grupo de objetivos de control y controles para la mitigación de los riesgos asociados y están alineados con ISO/IEC 27002. También indica los documentos y registros mínimos que debe contener para evidenciar el grado de funcionamiento del sistema. Aquí básicamente la guía define los criterios y metodología a seguir en sus cuatro etapas orientadas a cumplir los requisitos exigidos. En la fase DIAGNÓSTICO SGSI, la guía establece la forma de analizar el cumplimiento de la fase Planear de la norma frente a lo implementado en la organización, esto es fundamental para establecer la brecha y proyectar acciones orientadas a satisfacer todas las secciones de la norma, especialmente en el Capítulo SGSI, secciones Requisitos Generales, Establecimiento y Gestión. En sus demás capítulos la guía se orienta a modelar los procesos de valoración, tratamiento y monitoreo de riesgos donde se seleccionan controles estableciendo la forma de medir su efectividad, recomendando acciones según corresponda y estableciendo una valoración periódica de todo el proceso, temas tratados en las secciones de Implementación y Operación, Seguimiento y Revisión y Mantenimiento y Mejora del SGSI de la norma.

Respecto a la selección de objetivos de control y controles, la guía se basa en ISO/IEC 27002 ya que dicho estándar expone de manera detallada las buenas prácticas para asegurar los sistemas de información de una organización. Consta de 11 secciones, 39 objetivos de control asociados a cada área, y 133 controles que garantizan el cumplimiento de los objetivos. Para llegar a esta instancia, la guía establece que primero se realiza identificación y estimación de los riesgos, posterior ocurre la valoración, y luego se dan las pautas para su tratamiento. Los controles son seleccionados de esta norma según recomendaciones y criterios de la organización frente a la gestión del riesgo, sin embargo se contempla la incorporación de controles propios diseñados para situaciones particulares o inclusive tomados de otras metodologías. Mediante la declaración de aplicabilidad,

requisito obligatorio de ISO/IEC 27001, todos los anteriores son analizados justificando y documentando las razones para su selección o exclusión, es decir, ninguno queda sin revisión garantizando una completa exploración a posibles incidentes de seguridad.

Los procedimientos, actividades, análisis y resultados planteados en la guía sobre gestión del riesgo en la seguridad de la información son extraídas de ISO/IEC 27005 cuyo objeto de aplicación es proveer pautas y criterios sobre este aspecto. Sin embargo la norma no es una metodología específica, es muy general y corresponde a cada organización definir el enfoque según su naturaleza, eso sí, es aplicable a todo tipo de organización. Esta guía es una de muchas metodologías existentes bajo tal estructura camino a implementar un SGSI, pero recopila buenas prácticas producto de la experiencia de los autores. Esta norma al estar implícita en la guía ofrece continuidad, soporte y cumplimiento a ISO/IEC 27001 e ISO/IEC 27002. Alineado con ISO/IEC 27005, la guía cumple una serie de pasos en cada una de las actividades propuestas, las cuales en conjunto conforman el proceso de gestión del riesgo según lo muestra la figura 16.

El proceso es cíclico con el fin de redefinir sus fases ante un incidente o evento de seguridad que no fue controlado satisfactoriamente y para una actualización o revisión periódica preventiva de carácter obligatorio ajustándose a los cambios de la organización y del entorno. Esta característica determina un análisis en profundidad de los riesgos presentes y permite racionalizar los controles a implementar hasta llevar el riesgo a niveles aceptables por la organización. Se destaca en la figura 16 que las actividades están sujetas en todo momento a la divulgación a la alta Dirección y al personal involucrado. Las fases del proceso son:

- Establecimiento del contexto: Es la primera actividad donde inicia el proceso. Para su desarrollo es indispensable conocer muy bien la organización y contar con toda la información estratégica sobre el negocio. Así se definen los criterios básicos, se establece el alcance y límite y se define la estructura y responsabilidades para la gestión del riesgo en la compañía.

- Valoración del riesgo: Hacen parte de esta fase el análisis y la evaluación del riesgo. La primera incluye la identificación y la estimación del riesgo en las cuales se identifican activos de información, amenazas, vulnerabilidades y consecuencias. Por la otra parte se identifican escenarios incidentes y se

asignan valores a la probabilidad de ocurrencia y a las consecuencias de tales riesgos bajo criterios definidos en el contexto. La segunda etapa, también bajo criterios definidos en el contexto, determina el nivel del riesgo bajo una escala y permite priorizar su atención. Si toda la información anterior es suficiente para caracterizar los riesgos y determinar claramente las acciones a implementar en busca de niveles aceptables, la primera decisión del flujo llevará a la siguiente fase, de lo contrario se llevará a cabo otra iteración para redefinir actividades previas.

- Tratamiento del riesgo: En esta instancia se concretan las acciones a tomar sobre los riesgos valorados, es decir, se seleccionan los controles de acuerdo a lo planteado en el contexto según corresponda al objetivo y necesidades de la organización: reducir, retener, evitar o transferir el riesgo, lo anterior de acuerdo al costo de implementación de las opciones y los beneficios esperados. Si el tratamiento no es satisfactorio según lo esperado por la Compañía el segundo punto de decisión del flujo permite redefinir las etapas anteriores con las iteraciones que sean necesarias hasta lograr el riesgo residual o el nivel de riesgo que es aceptado para la Organización.

- Aceptación del riesgo: Esta actividad formaliza la declaración de la alta Dirección de la organización para asumir el riesgo residual o el riesgo tolerable con el fin de soportar y documentar las opciones de tratamiento, especialmente aquellas que por situaciones determinantes (por ejemplo altos costos) se omiten o posterga la implementación de controles, o sea, aquellos que no satisfacen los criterios normales definidos en el contexto. Es la parte final del ciclo normal y el siguiente paso es comunicarlo y monitorearlo.

- Comunicación del riesgo: Formaliza y divulga ante la alta Dirección, al personal involucrado en el proceso y ante la Organización en general, las actividades realizadas sobre la valoración y tratamiento del riesgo facilitando la toma de decisiones al ritmo de los cambios del negocio y al estado del SGSI. Esta etapa envía y/o recibe actualizaciones de cada fase del proceso según corresponda.

- Monitoreo y revisión del riesgo: Hace parte de la fase verificar del ciclo PHVA del SGSI. Considerando que los riesgos son cambiantes, esta actividad permite una alineación continua entre el proceso de gestión del

riesgo y los cambios que afectan la Organización y su entorno. Conforma la calidad y mejora continua del proceso.

A continuación se hace una descripción de cómo se alinea la guía con cada fase del ciclo PHVA.

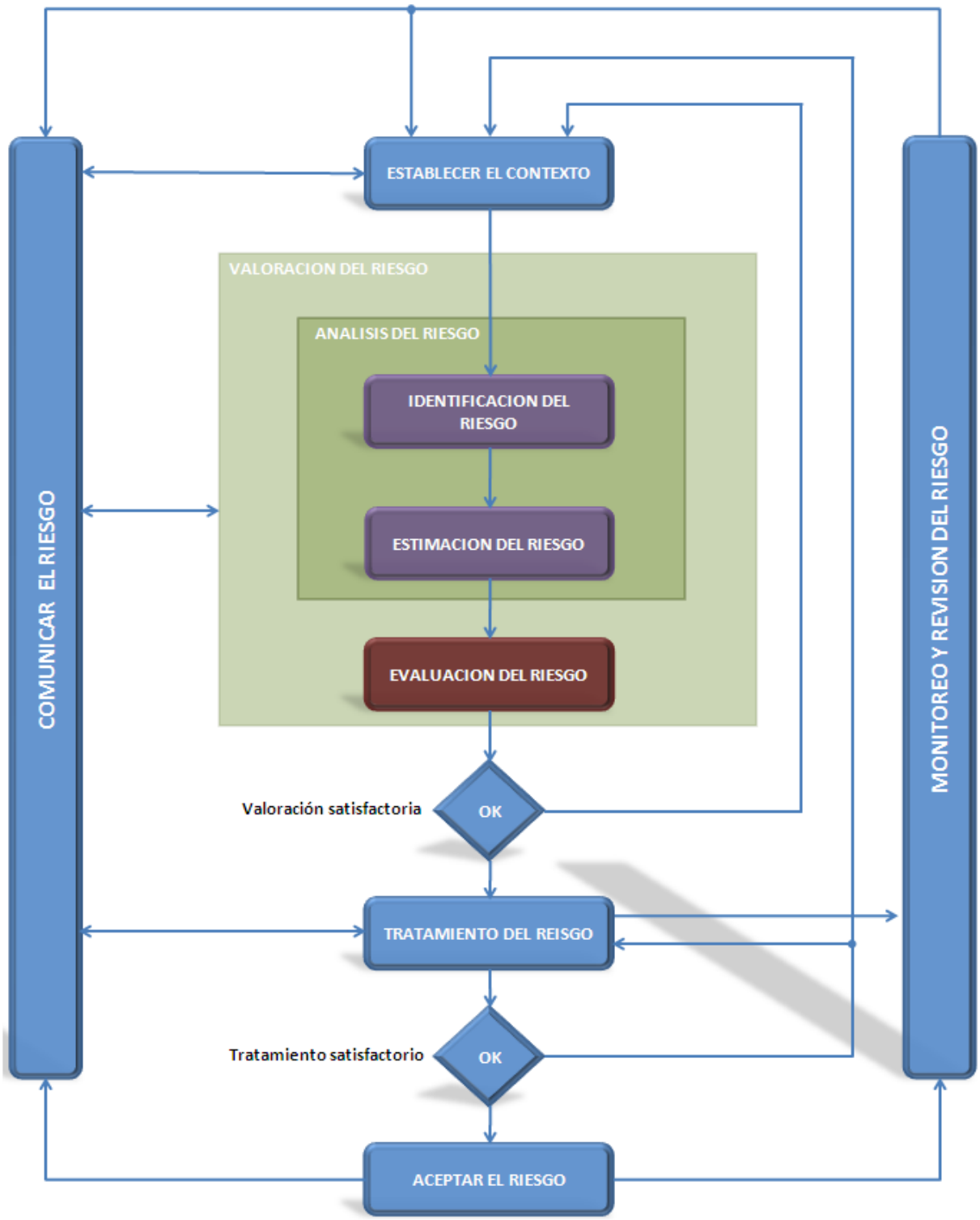
La guía plantea procesos de mejora continua involucrando interacciones hasta lograr reducción de los riesgos en niveles aceptables por la organización. Inicia con la planeación, donde se plantea un conocimiento detallado de la organización y sus requisitos de seguridad de la información como punto importante de partida para realizar los siguientes procesos:

- El diagnóstico. En el cual se examina el cumplimiento entre lo implementado en su SGSI y el estándar ISO/IEC 27001 de tal forma que permita conocer las actividades a gestionar para cumplir con lo exigido por el sistema. Este proceso determinará el estado de cumplimiento de la norma para las actividades incluidas en el mapa de procesos de la compañía y promueve el diseño de un modelo de gestión para llevarlas a un nivel de cumplimiento aceptable. Este será el punto de partida de la presente guía.

- Análisis, valoración, tratamiento, aceptación, comunicación y monitoreo de los riesgos. Se incluye como valor agregado y opcional la elaboración de un plan de continuidad del negocio.

Enseguida la fase Hacer abarca el tratamiento de riesgos, mediante las etapas monitoreo-revisión y comunicación del mismo se alcanza las fases verificar y actuar gracias a la medición de la eficacia de las medidas implementadas y a las interacciones cíclicas del proceso sobre acciones de mejora que permitirán inclusive redefinir la fase planear periódicamente o ante un incidente o evento de seguridad.

Figura 16: Proceso Gestión del Riesgo ISO/IEC 27005.



Fuente: Proyecto de Norma Técnica Colombiana NTC-ISO/IEC 27001.

A.2. ETAPA I: IDENTIFICACIÓN Y EVALUACIÓN PARA EL TRATAMIENTO DE LOS RIESGOS.

a. Reunir requisitos para esta actividad.

Validar que las fases análisis y diagnóstico SGSI y Organización de la Seguridad están cumplidas y documentadas.

b. Ejecutar acción.

1. Definir procesos que harán parte de la Gestión del Riesgo.

2. Definir requisitos de seguridad.

3. Asignar presupuesto, estimación de alto nivel de los recursos económicos y reservarlos con el fin de implantar y mantener el proceso de Gestión del Riesgo.

4. Valorar los Riesgos.

- Analizar los riesgos. En esta fase se encuentran, enumeran y se caracterizan los riesgos a los que se considera que está expuesta la organización.

  - Identificar activos de información.
  - Realizar análisis de estadísticas históricas sobre incidentes o eventos de seguridad.
  - Identificar los riesgos: Identificar amenazas, vulnerabilidades, consecuencias y controles existentes.
  - Estimar los riesgos: Asignar valores a la probabilidad de ocurrencia y a las consecuencias de un riesgo para estimar su valor en los posibles escenarios de incidentes aplicando el método ***Determinación del valor para la probabilidad y las consecuencias posibles de los riesgos.***

- Evaluar los riesgos.

  - Definir los criterios de clasificación del riesgo basados en las condiciones propias del negocio.
  - Filtrar la valoración de riesgos entregada por los dueños de los procesos para evitar subjetividad y reclasificarla si es necesario de acuerdo a los criterios definidos.
  - Priorizar los riesgos sobre los sistemas de la organización aplicando el concepto ***Organización = Sistema 1 + Sistema 2 + … + Sistema n.***
  - Comparar el riesgo estimado contra criterios de clasificación dados para determinar su importancia.

5. Alimentar la fase de comunicación del riesgo midiendo el alcance y restricciones al público destino.

6. Alimentar el plan de comunicación y sensibilización organizacional midiendo el alcance y restricciones al público destino.

c. Documentar resultados.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

A.3. ETAPA II: SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES.

a. Reunir requisitos para esta actividad.

Validar que la fase Valoración del Riesgo está cumplida satisfactoriamente y ha sido documentada.

b. Ejecutar Acción.

1. Plan de Continuidad del negocio (PCN). Si fue considerado por la alta dirección, definir, implementar y aprobar los procedimientos y estrategias que aseguren la continuidad oportuna y ordenada de los procesos críticos de la organización con niveles aceptables por los clientes. Se deben considerar las siguientes actividades:

   - Definir el proyecto.
   - Valorar los riesgos.
   - Asignar el tiempo objetivo de recuperación RTO.
   - Asignar el punto objetivo de recuperación RPO.
   - Diseñar el plan de estrategias.
   - Realizar la fase de pruebas, mantenimiento y mejora del proyecto.
   - Capacitar al grupo de trabajo, divulgar y sensibilizar toda la organización.
   - Realizar documentación final: gestión de incidentes, plan de emergencias, plan de comunicación de crisis, plan de recuperación de desastres.

2. Analizar si la valoración del riesgo fue satisfactoria.

   - Definir si luego de la primera iteración del flujo gestión del riesgo se cuenta con información suficiente para concretar en la siguiente fase las opciones de tratamiento que permitirán dejarlos en un nivel aceptable para la organización.
   - Definir si luego de la primera iteración del flujo gestión del riesgo es necesario otra iteración del flujo para redefinir el contexto.
   - Definir si se debe realizar otra iteración del flujo gestión del riesgo debido a revisión periódica del proceso cada seis meses o por un evento o incidente de seguridad no tratado satisfactoriamente.

3. Tratar los riesgos sobre los activos de información.

- Según resultado de la fase Evaluación del riesgo, se debe realizar un análisis de cumplimiento de los objetivos de control y controles listados en la norma ISO/IEC 27002 en el orden indicado: 5. POLÍTICA DE SEGURIDAD, 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, 13. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN, 14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO, 8. SEGURIDAD DE LOS RECURSOS HUMANOS, 11. CONTROL DE ACCESO, 15. CUMPLIMIENTO, 10. GESTIÓN DE COMUNICACIONES Y OPERACIONES, 12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN, 7. GESTIÓN DE ACTIVOS, 9. SEGURIDAD FÍSICA Y DEL ENTORNO, finalmente Objetivos relacionados a directrices propias para cubrir necesidades particulares que no estén incluidos en la norma, estos deberán clasificarse en un dominio afín de la norma para facilitar la trazabilidad.

- Determinar la totalidad de los controles nuevos, existentes y/o propios que son necesarios y contribuyen al cumplimiento de los objetivos de control.

- Determinar factor común de la totalidad de controles necesarios frente a los objetivos de control para evitar redundancia.

- Determinar compendio de la mejor alternativa de los controles en función de cumplimiento y costo-beneficio.

- Realizar un filtro a los controles seleccionados basado en las restricciones relacionadas.

- Justificar y documentar las razones por las cuales algún objetivo de control y/o controles listados en ISO/IEC 27002 son excluidos.

- Realizar análisis del presupuesto requerido para la implantación de los controles (existentes o planificados) sin ningún tipo de reserva o limite, fijando un periodo anual.

- Aprobación de la alta dirección por el presupuesto y listado definitivo de controles a implementar y mantener.

- Analizar si luego de esta decisión se presentan nuevos riesgos y por lo tanto se debe realizar una redefinición de todo el ciclo gestión del riesgo.

- Asignar responsable idóneo a cada control seleccionado.

- Generar documento Declaración de Aplicabilidad aprobado por la alta dirección.

- Aprobado por la alta dirección, proyectar la opción de tratamiento de riesgos a cada activo de información en orden de criticidad en función de los escenarios incidentes y el impacto al negocio según la fase evaluación del riesgo y según metodología establecida : 1. Retener, 2. Evitar, 3. Reducir, 4. Transferir, 5. Combinación de opciones.

- Definir indicadores para medida de eficiencia de los controles y metas a cumplir.

- Diseñar y realizar pruebas controladas a las salvaguardas para comprobar su rendimiento de forma preventiva.

- Diseñar registro de control al desempeño de los controles implantados.

- Recopilar y analizar los resultados parciales y/o finales de los indicadores de rendimiento de todos los controles.

- Documentar aprobación de la alta dirección sobre el riesgo residual obtenido luego del periodo de gestión del riesgo o si no cumple las expectativas de la organización, la autorización para revisar o redefinir las fases de gestión del riesgo que sean necesarias.

4. Alimentar la fase de comunicación del riesgo midiendo el alcance y restricciones al público destino.

5. Alimentar el plan de comunicación y sensibilización organizacional midiendo el alcance y restricciones al público destino.

c. Documentar resultados.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

A.4. ETAPA III: MEDICIÓN DE EFICACIA DE LOS CONTROLES.

a. Reunir requisitos para esta actividad.

Validar que la fase Tratamiento del Riesgo está cumplida satisfactoriamente y ha sido documentada.

b. Ejecutar acción.

1. Analizar si el plan de tratamiento del riesgo fue satisfactorio y es aceptado. Basado en los resultados de las fases identificación, estimación y evaluación del riesgo para el periodo bajo prueba o movido por un evento o incidente se seguridad, la alta dirección y el grupo SGSI debe analizar, documentar y aprobar:

- Cuáles riesgos tratados se han reducido a niveles aceptables y cumplen las expectativas de seguridad de las partes interesadas continuando así con las siguientes fases del proceso.

- Sobre los riesgos tratados pero que se mantienen en niveles intolerables, decidiendo si se debe redefinir solamente la fase de tratamiento o realizar varias iteraciones del ciclo hasta obtener resultados satisfactorio.

- Si se aceptan ciertos riesgos sin tratamiento o tratados pero por encima de niveles aceptables para la organización (por beneficios indirectos o costos de tratamiento demasiado altos) continuando así con las siguientes fases del proceso.

2. Alimentar la fase de comunicación del riesgo midiendo el alcance y restricciones al público destino.

3. Alimentar el plan de comunicación y sensibilización organizacional midiendo el alcance y restricciones al público destino.

c. Documentar resultados.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

A.5. ETAPA IV: SEGUIMIENTO, REVISIÓN Y VALORACIÓN PERIÓDICA DE RIESGOS.

a. Reunir requisitos para esta actividad.

Validar que la fase Tratamiento del Riesgo está cumplida satisfactoriamente y ha sido documentada.

b. Ejecutar acción.

1. Comunicar el riesgo.

- A través de un comité principal realizado por integrantes del grupo SGSI y con frecuencia mensual, generar un plan de comunicaciones que se aplique en cada instancia del flujo de gestión del riesgo de tal forma que permita al equipo de trabajo comprensión continua de las actividades, además de revisar avances, resultados, alinear y aclarar planes y decisiones entre el grupo SGSI, la alta dirección y los dueños de los procesos. Documentar y registrar actas de reunión.

- A través de un comité secundario realizado entre los dueños de los procesos y sus equipos de trabajo, donde se mide el alcance y las

restricciones para divulgar la información sobre el proceso de gestión del riesgo, dar continuidad a los objetivos del comité principal. Documentar y registrar actas de reunión.

- Las actas resultados de los comités deben contener acuerdos, planes de acción y de mejora, identificar responsables y niveles de escalamiento por las acciones definidas en los nuevos planes, ajustar y documentar conforme a las mejoras identificadas el proceso completo de gestión del riesgo, implementar las acciones acordadas, revisar el avance de implementación de los nuevos planes y del proceso en general.

2. Monitoreo y revisión del riesgo. Documentar acciones que evidencien la supervisión y redefiniciones del proceso de gestión del riesgo. Analizar los resultados y documentar las acciones tomadas de forma preventiva y correctiva frente a:

- Durante el periodo de ejecución definido para el proceso y en cada instancia del mismo.
- Ante un incidente o evento de seguridad.
- Ante cambios en el mapa de procesos de la organización.
- Ante modificación de los requisitos de seguridad.
- Reforma importante en el organigrama de la organización.
- Cambios en la asignación presupuestal para la gestión del riesgo.
- Valoración del riesgo no satisfactoria.
- Tratamiento del riesgo no satisfactorio.
- Indicadores de eficiencia de controles implantados.

3. Alimentar la fase de comunicación del riesgo midiendo el alcance y restricciones al público destino.

4. Alimentar el plan de comunicación y sensibilización organizacional midiendo el alcance y restricciones al público destino.

5. Consolidar Plan de Comunicación y Sensibilización Organizacional. Con los insumos recibidos por cada fase del proceso de gestión del riesgo, el grupo SGSI con el apoyo de las áreas de comunicación de la compañía realizan esta labor mediante campañas promotoras internas vía carteleras, intranet, correo electrónico, agenda en comités de área, etc. Se documentan todas las acciones tomadas al respecto en la carpeta del plan.

c. Documentar resultados.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

ANEXO B
PRUEBA PILOTO

GUÍA BASADA EN EL GRUPO DE NORMAS INTERNACIONALES ISO/IEC 27000 PARA GESTIONAR EL RIESGO Y SELECCIONAR CONTROLES EN LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Como parte del alcance del proyecto denominado MODELAMIENTO DE PROCESOS BASADOS EN EL GRUPO DE NORMAS INTERNACIONALES ISO/IEC 27000 PARA GESTIONAR EL RIESGO Y SELECCIONAR CONTROLES EN LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN del cual resulta la GUÍA BASADA EN EL GRUPO DE NORMAS INTERNACIONALES ISO/IEC 27000 PARA GESTIONAR EL RIESGO Y SELECCIONAR CONTROLES EN LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, se presenta a continuación la descripción de la prueba piloto que se realizó para validar la aplicabilidad y funcionalidad de la mencionada guía en una empresa de la región.

Para la aplicación de esta prueba piloto se estableció contacto con una Institución de orden nacional que hace presencia en la región y se obtuvieron las aprobaciones requeridas por parte de la Directora Regional para acceder a una parte de la información que se maneja en un área administrativa con el fin de utilizarla como insumo para la aplicación de la Guía de Gestión del Riesgo propuesta y con ello validar su utilidad en la implementación de un Sistema de Gestión de Seguridad de la Información.

La entidad cuenta con 33 Sedes Regionales y 206 Centros de atención a lo largo de todo el país en los cuales se atienden las solicitudes y se prestan los servicios a la población objetivo.

El funcionamiento general de la institución está enmarcado dentro del Mapa Procesos y procedimientos de la entidad. Dado que la Regional Risaralda se encuentra ya certificada en el Sistema de Gestión de Calidad bajo la norma ISO 9001, se pueden encontrar procedimientos oficiales que establecen las actividades que se deben llevar a cabo para el cumplimiento de una tarea específica, que para

el caso de la prueba piloto, servirán para identificar y medir el nivel de riesgo asociado a dichas actividades al ejecutarlas en el área definida.

Como política de seguridad, la entidad a nivel nacional, de dirección regional y en centros de atención está comprometido con la correcta administración y protección de la información propia de su actividad, trabajando en el aseguramiento de los datos cuya fuente son los macro procesos garantizando que sean consultados y/o modificados únicamente por personas autorizadas en el momento que se requiera. Para cumplir esta política, la organización cuenta con servidores públicos idóneos y con metodologías para valoración y tratamiento adecuado del riesgo.

Como alcance para la aplicación de esta prueba piloto, se elige la Regional Risaralda, teniendo en cuenta que esta regional no cuenta aún con un SGSI ya implementado y por consiguiente no tiene aún una certificación en ISO/IEC 27001, permitiendo así agregar valor a la empresa al aportar una guía que explique paso a paso las actividades exigidas por esta norma para realizar una efectiva gestión del riesgo como parte del proceso de certificación.

Con base en la autorización emitida desde la Dirección Regional para la aplicación de la prueba piloto, se obtuvo acceso a la información del *Proceso de Gestión Tecnológica* y sus procedimientos, ubicados dentro de los Macro procesos de Apoyo, para ser utilizados en la identificación, análisis y tratamiento de los riesgos del área de Planeación a nivel regional. Esta área se encarga, entre otras cosas, de hacer seguimiento y control a todos los indicadores de gestión de la entidad en la regional además de mantener la operación del Sistema Integrado de Gestión y ejecutar todas las actividades relacionadas con el seguimiento a las metas sociales y financieras fijadas en la vigencia para los programas tanto de Prevención como de Protección.

Una vez revisados los procedimientos que hacen parte del Proceso de Gestión Tecnológica, para la aplicación de la prueba piloto, se autorizó el acceso al procedimiento *PR15-MPA6 Manejo de Medios Removibles v1* aplicado al Grupo de Planeación y Sistemas Regional Risaralda. El procedimiento seleccionado es relativamente nuevo y surgió como respuesta ante la necesidad de oficializar las actividades y requisitos para el manejo de los medios removibles que son conectados a los equipos de cómputo de la entidad por parte de todos los colaboradores. Su objetivo es suministrar pasos a seguir cuando se deben almacenar datos en medios removibles buscando mantener la confidencialidad, Integridad y Disponibilidad de la información. El alcance de este procedimiento inicia con la socialización de la política de seguridad y finaliza con el cierre del

ticket asignado por la herramienta de gestión de la mesa de servicio. La metodología incorpora como criterio operativo, la obligación de cifrar los datos que se copien al medio removible. Los participantes son: usuario (funcionario o proveedor), jefe inmediato o supervisor de contrato y encargado de la seguridad.

Por otro lado las actividades incluidas en el procedimiento son:

- Dar a conocer la política de seguridad, G10 MPA6 Guía de Rotulado de la Información v2 y política de uso de medios removibles.

- Justificar la necesidad y aceptar la aplicación de políticas de uso de medios removibles y otras relacionadas, diligenciando el formato F1-PR15-MPA6 Carta de Aceptación Medios Removibles v1. En tal forma se resalta la necesidad de proteger los datos bajo un Sistema de Gestión de Seguridad de la Información, se exponen como prerrequisitos conocer la política de seguridad, el procedimiento PR15-MPA6 Manejo de Medios Removibles v1, la guía G10 MPA6 de Rotulado de la Información v2, la circular 014 de 22-Abr-10 sobre uso de recursos informáticos y el instructivo IT1 PR15 MPA6 para cifrar Información v1. También se hace responsable al funcionario por la seguridad de la información y por lo tanto asume las sanciones de ley aplicables al tema.

- Realizar la solicitud para autorización de uso de medios removibles generando el ticket en la mesa de servicio.

- Validar Si/No sobre el cumplimiento de requisitos de seguridad.

- Aprobar/Negar la solicitud.

- Documentar y cerrar el ticket.

El procedimiento *PR15-MPA6* será aplicado específicamente al área de Planeación Financiera donde se ejecuta el procedimiento *PR03.PE01 Procedimiento de Seguimiento Metas Sociales y Financieras v1* que pertenece al Proceso de Direccionamiento Estratégico y cuyo responsable en la zona es la Profesional de Apoyo Financiero del Grupo de Planeación y Sistemas. La razón de esta decisión se basa en que este es un procedimiento de aplicación regional bajo actividades que dependen de la gestión local del Grupo de Planeación y Sistemas,

caso contrario a otros procedimientos que requieren para su aplicación la participación de profesionales de la Sede Nacional de la entidad.

El *PR03.PE01* tiene como objetivo recolectar de forma sistemática los datos sobre el grado de cumplimiento en los centros zonales respecto a las metas y recursos comprometidos con los contratos y convenios suscritos con el fin de mejorar la calidad y oportunidad en la consolidación, análisis e implementación de correctivos necesarios para buscar la óptima ejecución de las metas sociales y financieras programadas en la Regional. Su alcance inicia con la elaboración y comunicación de las directrices generales y termina con la realimentación de la programación de metas sociales y financieras de la siguiente vigencia. Entre sus participantes se encuentran Dirección Financiera, Dirección de Información y Tecnología, Coordinador del Grupo Planeación y Sistemas, Profesional de Apoyo Financiero y Coordinador de Centro de atención.

Las actividades relevantes son:

- Elaborar directrices generales sobre programación de metas sociales y financieras.

- Recibir y comunicar a los Centros de Atención y Supervisores de Contratos las directrices generales e instrumentos para registrar, analizar y consolidar la información.

- Registrar mensualmente en el aplicativo definido en la organización: unidades de servicio, cupos, usuarios y costos ejecutados por municipios.

- Justificar liberación de saldos no ejecutados en los contratos asignados.

- Registrar mensualmente en el aplicativo definido en la organización modificaciones a las metas sociales y financieras.

- Analizar resultados obtenidos frente a las metas programadas y realizar cálculo de indicadores por proyecto.

- Realizar propuestas de mejora.

- Retroalimentar el proceso de programación de metas de la próxima vigencia.

En entrevistas con la profesional de Apoyo Financiero se detallaron las actividades propias del procedimiento, detectando que la información resultado de la aplicación del *PR03.PE01* es de carácter público y esta se registra, consolida y procesa en medios extraíbles durante la comunicación con los Centros de Atención (CA) y los Operadores (proveedores externos que ofrecen servicios a la entidad para cumplir su misión), considerando de esta forma incluso el correo electrónico donde se adjuntan los registros necesarios para el seguimiento. Su responsabilidad se ejecuta a lo largo del mes, iniciando cuando todos los CA registran en el Sistema de Información Misional SIM (el cual es la fuente oficial corporativa para realizar informes de gestión de uso interno y para presentar a las entidades de control) los datos sobre la ejecución de servicios y presupuesto. Esta información se consolida al final de este periodo en informes extraídos del aplicativo, en los análisis, propuestas de mejora y en la toma de decisiones realizados por el comité estratégico regional ampliado, conformado por la Directora Regional, los coordinadores de los CA y los coordinadores de los Grupos de Apoyo.

El seguimiento se realiza sobre dos metas del mapa estratégico, la misional y la financiera; y está definido en seis objetivos institucionales listados a continuación. Cada uno contiene varios proyectos los cuales abarcan diferentes servicios y estos incluyen cupos, unidades de servicio y beneficiarios:

- Lograr la atención integral de alta calidad a la población objetivo.
- Lograr el bienestar de la población objetivo.
- Ejecutar los recursos con la máxima eficiencia y efectividad.
- Incrementar la consecución de recursos.
- Lograr una organización apreciada por los colombianos que aprende y está orientada a resultados.

La Regional Risaralda está conformada por cinco CA cubriendo catorce municipios a saber:

- CA Pereira: atención en Pereira.
- CA Dosquebradas: cubre el municipio de Dosquebradas.
- CA Santa Rosa de Cabal: atiende usuarios en Santa Rosa de Cabal y Marsella.
- CA La Virginia: atiende La Virginia, Pueblo Rico, Apia, Santuario, La Celia y Balboa.

- CA Belén de Umbría: cobertura en Mistrató, Guática, Quinchía y Belén de Umbría.

Se evidencia que actualmente en el *PR03.PE01* no se aplica el *PR15-MPA6* ni la política de uso de medios extraíbles, la G10-MPA6 para rotulación de datos, tampoco se aplica control alguno a los activos de información.

Sobre la meta misional, se resaltan las siguientes actividades de control y supervisión a cargo de la profesional en la zona:

- Verificar que los CA y el Operador registren en los formatos definidos la información sobre ejecución de servicios en forma correcta cumpliendo las directrices impartidas por la sede nacional.

- Validar que los CA ingresen al SIM oportunamente la totalidad de registros requeridos (plazo hasta el octavo día del mes siguiente al evaluado).

- Con insumos provistos por los CA, registrar directamente en el SIM algunos servicios a cargo de la regional.

- Durante el periodo, para cada CA y para cada servicio, extraer y analizar informes del SIM relacionados con el cumplimiento de las metas programadas para generar alertas a los CA sobre baja ejecución y/o para abrir la posibilidad de ampliar cobertura de algunos servicios.

- Coordinar con los CA la corrección de registros hasta el noveno día del mes siguiente al evaluado.

- Asegurar que los CA ingresen la información definitiva, máximo el día diez de cada mes a las cinco de la tarde, último plazo dado por la sede nacional para registrar información usada para calcular los indicadores que demuestran las gestión regional.

- Recibir de la sede nacional solicitudes para corregir datos, acción necesaria para ajustar las metas de la próxima vigencia. Aunque se corrijan estos datos, no se modifican los indicadores que se reportaron en el plazo inicial establecido.

- Extraer informes definitivos del SIM, consolidar, analizar y realizar propuestas de mejora en comité estratégico regional ampliado.

Respecto a la meta financiera corresponde:

- Seguimiento servicio a servicio, sobre todo el presupuesto asignado a la regional basada en la información que envían los profesionales financieros de cada CA.

- Consolidar a nivel de proyecto, la ejecución presupuestal.

- Cruzar la ejecución contra el cierre presupuestal de cada proyecto reportado en el Sistema Integrado de Información Financiera (SIIF) donde reposa el estado de la ejecución de todas las entidades estatales el cual es administrado por el Ministerio de Hacienda.

- Reportar y justificar a la sede nacional las situaciones que afectaron la ejecución del presupuesto.

- Extraer informes definitivos del SIM, consolidar, analizar y realizar propuestas de mejora en comité estratégico regional ampliado.

Surge una tercera acción a cargo de la profesional de la zona, derivada de las actividades de seguimiento mencionadas y corresponde a gestionar en el SIM las modificaciones de las metas sociales y financieras en curso. Resulta que la regional puede trasladar cupos de un servicio a otro, solicitar cupos y recursos adicionales o ejecutar más de lo contratado con el Operador a pesar que no haya sido programado y presupuestado.

B.1. APLICACIÓN DE LA GUÍA PROPUESTA PARA LA GESTIÓN DEL RIESGO

ETAPA I: Identificación y Evaluación para el Tratamiento de los Riesgos

1. Requisito:

Compromiso de la alta Dirección para realizar el diagnóstico. Dado que se trata de una prueba piloto aplicada a los procedimientos y en el área autorizada por la Institución, se toma dicha autorización como la aprobación de la dirección para realizar el diagnóstico inicial que mida el grado de cumplimiento actual de los requisitos de seguridad según la norma ISO 27001, teniendo en cuenta que ya se cuenta con un Sistema de Gestión de Calidad (SGC) implementado y certificado bajo la norma ISO 9001, el cual ha definido oficialmente el proceso de Gestión Tecnológica que será objeto de análisis y aplicación en esta prueba piloto.

Según las condiciones de esta prueba, la coordinadora del Grupo de Planeación y Sistemas asigna a la profesional encargada del mantenimiento del SGC en la regional y al ingeniero líder de sistemas para apoyar a los ejecutores con la información que sea requerida y para el seguimiento y control según el alcance de la prueba.

1.1 Diagnóstico Inicial del SGSI en la Organización.

Como primer paso para el análisis y evaluación de los riesgos, con el apoyo del ingeniero de sistemas regional se califica cada aspecto relacionado en el formato para el diagnóstico inicial del SGSI en la compañía según la metodología planteada en la guía y del cual se obtienen los siguientes resultados:

Sub Fase	Sumatoria Calificaciones Obtenidas	Sumatoria Máxima Posible	Porcentaje Avance
Planear-Planear	188	300	62,7%
Planear-Hacer	16	40	40,0%
Planear-Verificar	17	32	53,1%
Planear-Actuar	9	16	56,3%

Para determinar el porcentaje de avance del primer aspecto tocado por ISO/IEC 27001 llamado SGSI y que corresponde a la fase Planear del ciclo PHVA, basta con multiplicar el avance de cada una de las cuatro sub fases por el 25% y sumar los resultados, obteniendo así que dicho porcentaje de avance de esta fase es el **53%.**

Teniendo en cuenta que la anterior calificación corresponde a uno de los cinco aspectos que componen la norma ISO/IEC 27001, el porcentaje de avance respecto a la implementación de todo el SGSI es: 53% * 20% = **10,6%.** Se debe recordar que el alcance de la guía es la fase Planear y no aborda las otras cuatro, sin embargo la entidad sí ha realizado gestión sobre ellas y por lo tanto el estado de implementación del SGSI será mayor solo que no se reflejará en la guía por lo antes aclarado.

1.2 Análisis del Diagnóstico.

Hallazgos:

SGSI-P-P-01: No se ha asignado al personal suficiente para la implementación del SGSI en la organización.

SGSI-P-P-02: No se ha definido un documento oficial de declaración de la dirección para la implementación del SGSI en la organización.

SGSI-P-P-03: No se ha definido un Comité de Gestión SGSI ni documento de Organización de la Seguridad.

SGSI-P-P-04: No se ha definido un procedimiento claro para la divulgación, sensibilización y capacitación del personal de la organización frente a los avances del SGSI y su aplicación.

SGSI-P-P-05: En el inventario de activos de información no se incluyeron los activos intangibles.

SGSI-P-P-06: No se han identificado las dependencias entre activos de información que ayude a identificar activos críticos.

SGSI-P-P-07: No existe documento completo ni oficial para análisis y valoración de riesgos.

SGSI-P-P-08: No está definido claramente un proceso de gestión del riesgo que incluya criterios de aceptación de riesgo residual.

SGSI-P-P-09: La Declaración de Aplicabilidad no justifica los objetivos de control y controles seleccionados y no seleccionados.

SGSI-P-P-10: Los procedimientos del Plan de Continuidad del Negocio no han sido divulgados ni puestos a prueba.

SGSI-P-H-01: No existen documentos guías para la ejecución del Plan de Tratamiento de Riesgos.

SGSI-P-H-02: No existen indicadores de eficacia y eficiencia de los controles implementados.

SGSI-P-H-03: No se han definido procedimientos ni controles adicionales para reaccionar ante incidentes de seguridad presentados en la fase HACER.

SGSI-P-H-04: No existe informe de implementación de controles y resultados.

SGSI-P-V-01: No se realizan revisiones periódicas por la Dirección de los informes de los responsables de la seguridad.

SGSI-P-V-02: No se realizan análisis periódicos de la definición de riesgos residuales o aceptables.

SGSI-P-A-01: No se generan informes consolidados de atención y solución a las acciones correctivas – preventivas.

SGSI-P-A-02: No se hace un seguimiento riguroso de las soluciones a las acciones correctivas – preventivas.

1.3 Organización de la Seguridad.

Creación del grupo SGSI: enfocado a los procedimientos bajo análisis de forma local, la Coordinadora del grupo Planeación y Sistemas de la Regional Risaralda realizó reunión con los integrantes del grupo donde se declara el apoyo a la prueba piloto sobre el procedimiento PR15-MPA6 Manejo de Medios Removibles-v1 aplicado al área de Planeación Financiera, particularmente al procedimiento *PR03.PE01 Procedimiento de Seguimiento Metas Sociales y Financieras v1;* en ella también se conforma el grupo SGSI asignando funciones y responsables así:

- Como responsable de la seguridad, el ingeniero líder del grupo de sistemas, encargado de coordinar la forma de actuar ante eventos y/o incidentes de seguridad.

- El Comité de Gestión queda conformado por la profesional que coordina la Estrategia Permanente de Innovación y Cambio Organizacional (EPICO) en la regional, la profesional de Apoyo Financiero y el ingeniero Líder del Grupo de Sistemas. Quedan encargados de controlar la ejecución del proceso y aplicar las acciones correspondientes.

- El Comité de Dirección fue delegado por la Directora Regional quien tiene las facultades de aprobar el apoyo a la aplicación de esta prueba piloto en la entidad a nivel regional, dejando a cargo de este rol a la Coordinadora del grupo Planeación y Sistemas como responsable de tomar las decisiones de alto nivel frente a la seguridad de la información ya que los procedimientos y área de aplicación seleccionados son competencia de este grupo.

1.4 **Plan de Continuidad del Negocio**.

El resultado del análisis del grupo SGSI indica que los procedimientos seleccionados no tienen un nivel de criticidad que justifique incluirlos en el Plan de Continuidad del Negocio PCN, así mismo, dado el alcance de la prueba piloto. Otra razón que justifica esta acción es que la entidad ya tiene definida la guía *G6-MPA6 Gestión Continuidad del Negocio v1* donde están identificados los procesos y activos críticos como también los tiempos de recuperación y planes de acción, y de los cuales no hacen parte los procedimientos seleccionados en la prueba piloto.

1.5 **Acuerdos de confidencialidad**.

La entidad establece acuerdos de confidencialidad firmados por los ejecutores de la prueba piloto como medida de seguridad al intercambio de información con agentes externos a la organización. En relación a la gestión del riesgo sobre los procedimientos bajo análisis, se define que no aplica con proveedores externos ya que la información manejada es de carácter público y sólo demuestra gestión de la regional, es propia de las funciones de cada área y no se revela información clasificada.

1.6 Comunicar el riesgo.

En esta instancia, se cumple el primer insumo la fase de comunicación del riesgo de ISO/IEC 27005 donde se sensibiliza, comunica y formalizan las decisiones y resultados a los dueños de los procesos.

1.7 Sensibilización y comunicación.

Para diseñar el plan de comunicaciones hacia la organización en busca de crear una cultura de seguridad de la información, queda designada la profesional EPICO. Sin embargo el grupo SGSI define que para la prueba piloto no se pone en marcha ya que se detecta como riesgo generar confusión a los diferentes grupos de la regional debido a las actividades propias del sistema integrado de gestión.

2. ACCIÓN

2.1 Definir Procesos que harán parte de la Gestión del Riesgo.

Tomando como base el Sistema de Gestión de Calidad en el cual están definidos los procesos y procedimientos que componen la organización y teniendo en cuenta la autorización otorgada para la aplicación de esta prueba piloto, se definió que el proceso sobre el cual se aplicará la guía para la gestión del riesgo propuesta será el de ***Gestión Tecnológica*** ubicado dentro de los Macro procesos de Apoyo. Dentro de este proceso, se determinó que el procedimiento sobre el cual se realizará la gestión de riesgos, según el alcance de la prueba piloto, será el ***PR15-MPA6 Manejo de Medios Removibles v1*** aplicado al Grupo de Planeación y Sistemas Regional Risaralda particularmente al área de Planeación Financiera sobre el procedimiento ***PR03.PE01 Procedimiento de Seguimiento Metas Sociales y Financieras v1***.

2.2 Definir requisitos de Seguridad. En reunión sostenida por el Comité de Gestión se definen los siguientes aspectos a tener en cuenta para proteger los activos de información del área Planeación Financiera según los procedimientos seleccionados, todos relacionados al proceso de Gestión Tecnológica dentro del marco corporativo y como área interesada el Grupo de Planeación y Sistemas Regional Risaralda. De esta forma se cumple la fase comunicar el riesgo.

Cuadro 2: Requisitos de Seguridad Prueba Piloto.

REQUISITO DE SEGURIDAD	LEY ASOCIADA	CONSECUENCIAS
Integridad y disponibilidad de la información.	Misión, Visión, Objetivos Institucionales, Política de seguridad.	- Afectación a los objetivos institucionales. - Afectación a la sociedad. - Baja calidad y cobertura en los servicios prestados. - Incumplimiento marco legal constitucional. - Afectación de imagen corporativa. - Incumplimiento de metas sociales y financieras. - Pérdida de eficiencia en el uso de recursos y presupuesto.
Calidad de la información registrada por los CA.	Misión, Visión, Objetivos Institucionales.	
Autenticidad y control de acceso en la información enviada por los CA.	Objetivos Institucionales, Política de seguridad.	
Autenticidad y control de acceso al aplicativo SIM.	Objetivos Institucionales, Política de seguridad.	
Cumplir niveles de servicio para entrega de reportes de seguimiento a los CA.	Misión, Visión, Objetivos Institucionales.	
Calidad en análisis y propuestas de mejora en busca de cumplimiento de las metas propuestas.	Misión, Visión, Objetivos Institucionales.	
Cumplir niveles de servicio en programación y ejecución de metas sociales y financieras de la vigencia actual y próxima.	Misión, Visión, Objetivos Institucionales.	
No afectar los indicadores de gestión de la regional.	Objetivos Institucionales.	

2.3 Asignar presupuesto.

El grupo SGSI determina que existen los recursos tanto económicos, técnicos y humanos para implantar y mantener el proceso de gestión de riesgo sobre el área y procedimientos escogidos, de tal forma que no es necesario obtener presupuesto adicional. La entidad cuenta con plataformas centralizadas como por ejemplo la consola de antivirus, también existen procedimientos y políticas entre ellas las copias de respaldo. Por otro lado, los profesionales del Grupo de Planeación y Sistemas Regional Risaralda han conformado el grupo SGSI para la prueba piloto, y el área de Sistemas está encargada de dar soporte sobre aspectos específicos y supervisar la aplicación y seguimiento de los procedimientos. Por último, la operación y parte de la administración de la información se ha tercerizado mediante el Contrato con una Unión Temporal como proveedor.

2.4 Valoración de riesgos.

2.4.1 Análisis de Riesgos

a. Identificación de activos.

En reunión sostenida entre el Comité de Gestión y el responsable del procedimiento *PR03.PE01,* cumpliendo así de una vez con la fase comunicación del riesgo, se identifican las funciones de cada uno en el procedimiento y se define que la Profesional de Apoyo Financiera es el rol propietario y responsable de los activos de información. También se valida la aplicación de la metodología propuesta por la guía por parte del dueño del procedimiento y se realiza el filtro definitivo a la identificación y valoración de los activos que son clave para el desarrollo de los objetivos del área. En el cuadro 3 se muestran los resultados.

Se resalta las dependencias encontradas entre los activos primarios de tipo información, ya que se identifican varios registros que son comunes a otros activos y a las amenazas y vulnerabilidades encontradas; es así como se clasifica un solo activo primario tipo información en forma genérica llamado *REPORTES Y REGISTROS DE INFORMACIÓN* que contiene:

- Reporte preliminar de seguimiento y análisis.

- Registro de servicios reportados por la regional.
- Análisis mensual de la ejecución presupuestal.
- Análisis mensual de la ejecución meta misional.
- Actas de comité ampliado.
- Programación metas sociales y financieras próxima vigencia.

Cuadro 3: Identificación y valoración de activos, amenazas y vulnerabilidades sobre el procedimiento PR03.PE01.

Etiquetas de fila	CODIGO ESCENARIO	DOMINIO AMENAZA	AMENAZA	DOMINIO VULNERABILIDAD	VULNERABILIDAD
EQUIPO DE COMPUTO	**66_PlaF-003**	Fallas técnicas	**Falla en equipo de computo**	Técnico	Falta de mantenimiento
	66_PlaF-004	Fallas técnicas	**Falla en equipo de computo**	Técnico	Error en soporte técnico
	66_PlaF-005	Compromiso de la información	**Robo, vandalismo**	Personal	Falta de activación sistema de alarma en oficina
	66_PlaF-006	Compromiso de la información	**Robo, vandalismo**	Lugar	Ubicación en área de oficina susceptible a robo
RECURSO HUMANO	**66_PlaF-001**	Acciones no autorizadas	**Ingreso intencional de datos falsos o corruptos**	Personal	Empleado insatisfecho
	66_PlaF-002	Compromiso de las funciones	**Error involuntario en registro de datos**	Personal	Aplicación inadecuada de procedimientos
REPORTES Y REGISTROS DE INFORMACION	**66_PlaF-007**	Compromiso de la información	**Perdida de información**	Personal	No se aplica el procedimiento copias de respaldo
	66_PlaF-008	Fallas técnicas	**Errores de procesamiento en aplicación SIM**	Software	Especificaciones incompletas para el desarrollo
	66_PlaF-009	Fallas técnicas	**Errores de procesamiento en aplicación SIM**	Software	Sobrecarga de procesamiento en servidor
	66_PlaF-010	Acciones no autorizadas	**Acceso no autorizado**	Personal	No se aplica PR15-MPA6, G10 MPA6.
	66_PlaF-011	Compromiso de la información	**Virus**	Software	BD definición de virus desactualizada
	66_PlaF-012	Compromiso de la información	**Virus**	Personal	No se aplica PR15-MPA6
	66_PlaF-013	Perdida de servicios esenciales	**Falla de servicios de telecomunicaciones**	Red	Punto único de falla en red del proveedor
	66_PlaF-014	Perdida de servicios esenciales	**Falla de servicios de telecomunicaciones**	Red	Línea de comunicaciones sin protección en red del proveedor
	66_PlaF-015	Perdida de servicios esenciales	**Falla plataforma telefonía IP**	Red	Punto único de falla en red del proveedor
	66_PlaF-016	Perdida de servicios esenciales	**Falla plataforma telefonía IP**	Red	Línea de comunicaciones sin protección en red del proveedor
	66_PlaF-017	Perdida de servicios esenciales	**Falla plataforma telefonía IP**	Red	Soporte técnico deficiente

b. Estadísticas históricas sobre incidentes o eventos de seguridad.

En la reunión del comité de gestión se analiza que no han ocurrido eventos o incidentes de seguridad sobre el área y procedimiento bajo análisis.

c. Identificar los riesgos.

En esta sesión de trabajo el comité identifica y valora amenazas y vulnerabilidades como también detecta controles existentes. Se identifican diez (10) amenazas agrupadas en cinco (5) dominios a saber: acciones no autorizadas, compromiso de la información, compromiso de las funciones, falla técnica y pérdida de servicios esenciales. Estas amenazas están relacionadas a las vulnerabilidades de los activos de información correspondientes, conformando así diecisiete (17) escenarios incidentes. En el cuadro 4 se muestra el cruce de las variables respectivas evidenciando que no hay amenazas comunes sobre los activos, sin embargo hay vulnerabilidades en los dominios *Personal* y *Red* que afectan varios activos y están relacionadas con la arquitectura de telecomunicaciones del proveedor, con la falta de aplicación del PR15-MPA6 y ejecución errada del PR03.PE01.

Los controles existentes que aplican a los escenarios incidentes son:

- Contrato con Unión Temporal para la operación y parte de la administración de la información.
- Sistema de alarma de seguridad en la oficina del Grupo Planeación y Sistemas.
- Disponibilidad de un procedimiento para realizar copias de respaldo a la información de los usuarios.
- PR15-MPA6 Manejo de Medios Removibles v1.
- G10 MPA6 Guía de Rotulado de la Información.
- PR03.PE01 Procedimiento de Seguimiento MSYF v1.
- Política de seguridad.

d. Estimar los riesgos.

En la misma reunión, el Comité de Gestión y la propietaria de los activos, aplicando los criterios descritos en la guía, calculan la probabilidad de ocurrencia y criticidad del Riesgo sobre el Activo para todos los escenarios incidentes. En esta instancia se encuentra que los riesgos estimados tienen consecuencias media-alta (valorados con nivel 5 hasta 8), que el recurso humano y los registros de información son los activos más importantes y los que presentan más escenarios de riesgo.

Cuadro 4: Estimación de riesgos sobre el procedimiento PR03.PE01.

Etiquetas de fila	ACTIVO	AMENAZA	VULNERABILIDAD
5	REPORTES Y REGISTROS DE INFORMACION	Falla plataforma telefonía IP	Línea de comunicaciones sin protección en red del proveedor
			Punto único de falla en red del proveedor
			Soporte técnico deficiente
6	EQUIPO DE COMPUTO	Falla en equipo de computo	Error en soporte técnico
			Falta de mantenimiento
		Robo, vandalismo	Falta de activación sistema de alarma en oficina
			Ubicación en área de oficina susceptible a robo
7	RECURSO HUMANO	Ingreso intencional de datos	Empleado insatisfecho
	REPORTES Y REGISTROS DE INFORMACION	Acceso no autorizado	No se aplica PR15-MPA6, G10 MPA6.
		Errores de procesamiento en aplicación SIM	Especificaciones incompletas para el desarrollo
			Sobrecarga de procesamiento en servidor
		Falla de servicios de telecomunicaciones	Línea de comunicaciones sin protección en red del proveedor
			Punto único de falla en red del proveedor
		Perdida de información	No se aplica el procedimiento copias de respaldo
		Virus	BD definición de virus desactualizada
			No se aplica PR15-MPA6
8	RECURSO HUMANO	Error involuntario en registro de datos	Aplicación inadecuada de procedimientos

2.4.2 Evaluar los riesgos.

En el mismo comité, el grupo SGSI filtra los criterios de clasificación del riesgo establecidos por la Profesional de Apoyo Financiero. Sustentada en el análisis de requisitos de seguridad del Grupo Planeación y Sistemas regional Risaralda determina que según la estimación de riesgos realizada:

- Se clasifica un riesgo de alta importancia si se materializa sobre una relación escenario-activo con valoración mayor o igual a siete (7), así mismo será media importancia seis (6) y baja importancia cinco (5).

De igual forma, se establece la categoría si al materializarse un riesgo ya identificado en el proceso, se afecta el cumplimiento de los indicadores que reflejan la eficiencia en cubrir cupos, usuarios y servicios en toda la regional e impacta las labores de todos los grupos de apoyo que la conforman.

- Se clasifica un riesgo de alta importancia si por la materialización de una relación escenario-activo, la meta del indicador Regional ***MPE1-01: Porcentaje de cumplimiento de la meta frente a la ejecución presupuestal en compromisos*** se da < 95%, 95% ≤ importancia media ≤ 98% y bajo si es > 98%.

- Un riesgo será alto si la meta del indicador ***MPE1-02: Porcentaje de cumplimiento de la meta frente a la ejecución presupuestal en obligaciones*** se cumple < 95%, 95% ≤ importancia media ≤ 98% y bajo si es > 98%.

- Un riesgo será alto si la meta del indicador ***MPE1-04: Porcentaje de ejecución de metas sociales de los programas misionales correctivos*** se cumple <70%, 70% ≤ importancia media ≤ 90% y bajo si es > 90%.

- Un riesgo será alto si la meta del indicador ***MPE1-05: Porcentaje de ejecución de metas sociales de programas misionales preventivos*** se cumple <70%, 70% ≤ importancia media ≤90% y bajo si es > 90%.

El riesgo aceptable por el Grupo Planeación y Sistemas Regional Risaralda se dará si al materializarse los escenarios incidentes sobre los activos y al aplicarse los objetivos de control y controles en la fase de tratamiento, cualquier meta de los indicadores Regionales se cumple en un nivel bajo.

La siguiente definición realizada por el comité fue la priorización de los riesgos. Se identificó un solo sistema llamado ***PR03.PE01 Procedimiento de Seguimiento MSYF v1*** con una peso de 110 y según el método sugerido en la guía, se da una nueva valoración a los activos de información que permite dar la importancia al interior del proceso según el siguiente orden de atención: reportes y registros, equipo de cómputo y recurso humano. En el cuadro 5 se muestran los resultados.

Cuadro 5: Orden de Importancia de los activos y peso del sistema PR03.PE01.

Nuevo valor del activo	ACTIVO	Suma de Valor activo vs Pi escenario
15	RECURSO HUMANO	15
24	EQUIPO DE COMPUTO	24
71	REPORTES Y REGISTROS DE INFORMACIÓN	71
Total general		**110**

ETAPA II: Selección de objetivos de control y controles.

1. Requisito

En una nueva reunión donde participan el comité de gestión y la alta dirección, se valida que la fase Valoración del Riesgo sobre los activos relacionados con la seguridad de la información está cumplida satisfactoriamente y ha sido documentada. Al estar presentes todos los involucrados en el proceso de gestión del riesgo, se da por cumplida la comunicación del riesgo hasta esta instancia tanto para la etapa I como la etapa II.

2. Acción

2.1 Valoración satisfactoria del riesgo

El grupo SGSI encuentra que para la fase Planear, alcance de esta guía, se cuenta con toda la información que permite proyectar estrategias para tratar los escenarios incidentes llevándolos a niveles aceptables por la organización de tal forma que se declara cumplimiento exitoso en la valoración realizada en la etapa I del proceso. Si se implementan las otras fases del ciclo PHVA, esta revisión se dará cada seis meses o motivada por ocurrencia de incidentes, eventos de seguridad o cambios en la estructura de la organización.

2.2 Tratamiento de riesgos sobre los activos de información

Según aplicación de la guía, el Comité de Gestión y la Alta Dirección establecen los objetivos de control y controles definitivos y consolidan la declaración de

aplicabilidad. Para llegar a este resultado se aplica la metodología en el orden definido:

- Validar el cumplimiento de los objetivos de control según el orden planteado. Se Justifica cuáles deben cumplirse y cuáles no, según aplican al procedimiento analizado.

- Se identifican sin restricción alguna los controles que contribuyen al cumplimiento del punto anterior.

- Se realiza un filtro para encontrar el factor común en los controles que aplican a los objetivos seleccionados buscando la mejor alternativa.

- Se analizan las restricciones que presentan los controles y que limitan su aplicación.

- Se identifica que todos los controles necesarios existen dentro de la entidad y por lo tanto no aplica un análisis de presupuesto. Se obtienen veintisiete (27) salvaguardas como listado definitivo relacionados a nueve (9) Dominios, veinte (20) Objetivos de Control y cincuenta y siete (57) Controles de la norma.

- Dieciséis (16) salvaguardas relacionados con políticas, procesos, procedimientos, o instructivos que contribuyen a veinte (20) objetivos de control entre los dominios: *5. Política de Seguridad*, *6.Organizacion de la Seguridad de la información*, *7. Gestión de Activos*, *8. Seguridad de los Recursos Humanos*, *9. Seguridad Física y del Entorno*, *10. Gestión de Comunicaciones y Operaciones* y *11. Control de Acceso, 12. Adquisición, desarrollo y mantenimiento de sistemas de información* y *13. Gestión de los Incidentes de la Seguridad de la Información*.

- Por otro lado, diez (10) salvaguardas de orden técnico apuntan hacia los dominios: *9. Seguridad Física y del Entorno (*Objetivos: *9.1 Áreas Seguras, 9.2 Seguridad de los Equipos), 10. Gestión de Comunicaciones y Operaciones (*Objetivo: *10.10 Monitoreo)* y *11. Control de Acceso (*Objetivo: *11.6 control de acceso a las aplicaciones y a la información).*

- Finalmente una salvaguarda como plan de capacitación asiste el objetivo *8.2 Durante la Vigencia del Contrato Laboral* del dominio *8. Seguridad de los Recursos Humanos.*

- Se identifica que los dominios presentes son comunes para todos los activos y que varios controles protegen más de un activo sin redundancia. Por ejemplo, el PR15 MPA6 cubre tres (3) dominios, cinco (5) objetivos de control y diez (10) controles de la norma y en todos los casos es aplicable.

- Se documenta en la Declaración de Aplicabilidad y queda controlada a cargo de la Profesional EPICO.

Basados en el resultado obtenido, el comité declara que se pueden enfrentar los riegos con la disponibilidad y profundidad requerida por la organización.

El comité de dirección conformado por la Coordinadora del Grupo Planeación y Sistemas designa a la Profesional de Apoyo Financiero, Profesional EPICO, Líder del Grupo Sistemas y ella misma como los responsables de los controles según se documenta en la declaración de aplicabilidad.

Ahora, de acuerdo a lo recomendado en la guía, se muestra en el cuadro 6 el análisis de las opciones de tratamiento de riesgos proyectadas realizado por el comité SGSI y aprobado por la alta Dirección. Se analizará posteriormente si serán socializados los riesgos transferidos a las áreas externas designadas como responsables.

Cuadro 6: Análisis de tratamiento de riesgos en PR03.PE01

Etiquetas de fila	CODIGO ESCENARIO	CONTROL ASOCIADO	JUSTIFICACION TRATAMIENTO
RETENER	**66_PlaF-002**	Plan de capacitación, Grupos de estudio y trabajo, Comunicaciones institucionales	La capacitación y grupos de estudios se realizan de forma mensual y se complementa con los comités básicos y ampliados.
	66_PlaF-005	Sistema de alarma en oficina	El control existe y funciona bien, se exige a los funcionarios de parte de la Coordinadora del Grupo Planeación y Sistemas el uso obligatorio y se cuenta con el apoyo de otro control como el contrato de vigilancia privada para la sede.
	66_PlaF-007	Plan de capacitación, Grupos de estudio y trabajo, Comunicaciones institucionales	La capacitación y grupos de estudios se realizan de forma mensual y se complementa con los comités básicos y ampliados.
	66_PlaF-010	Plan de capacitación, Grupos de estudio y trabajo, Comunicaciones institucionales	La capacitación y grupos de estudios se realizan de forma mensual y se complementa con los comités básicos y ampliados.
	66_PlaF-012	Plan de capacitación, Grupos de estudio y trabajo, Comunicaciones institucionales	La capacitación y grupos de estudios se realizan de forma mensual y se complementa con los comités básicos y ampliados.
RETENER-TRANSFERIR	**66_PlaF-001**	Proceso de control interno disciplinario	El proceso esta reflejado en el contrato del funcionario, además es conocido por toda la organización y es efectivo. Lo inicia la Coordinadora del Grupo Planeación y Sistemas pero se desarrolla a cargo de la oficina de control interno disciplinario.
	66_PlaF-003	Programa nacional de mantenimiento a equipos de computo.	El grupo de sistemas regional no tiene la capacidad de cubrir el programa totalmente, se transfiere a la Dirección de Información y Tecnología para que gestione contrato con proveedor.
	66_PlaF-004	Contrato con Unión Temporal.	El proveedor es responsable contractualmente por garantizar su trabajo y es controlado y supervisado por la Dirección de Información y Tecnología.
	66_PlaF-006	Sistema de alarma en oficina / Contrato de vigilancia privada para la sede	El control existe y funciona bien, se exige a los funcionarios de parte de la Coordinadora del Grupo Planeación y Sistemas el uso obligatorio y se cuenta con el apoyo de otro control como el contrato de vigilancia privada para la sede
TRANSFERIR	**66_PlaF-008**	Procedimientos de desarrollo de Software	El control existe y funciona bien pero no es responsabilidad del Grupo Planeación y Sistemas por ello se transfiere al responsable Fabrica Software en sede nacional
	66_PlaF-009	Monitoreo rendimiento de Bases de Datos	El control existe y funciona bien pero no es responsabilidad del Grupo Planeación y Sistemas por ello se transfiere al responsable Subdirección de Sistemas de información.
	66_PlaF-011	Consola de gestión de antivirus	El control existe y funciona bien pero no es responsabilidad del Grupo Planeacion y Sistemase por ello se tranwfiere al respnsable Subdireccion de Sistemas de informacion.
	66_PlaF-013	Contrato con Unión Temporal.	El control existe y funciona bien pero no es responsabilidad del Grupo Planeación y Sistemas por ello se transfiere al responsable Dirección de Información y Tecnología.
	66_PlaF-014	Contrato con Unión Temporal.	El control existe y funciona bien pero no es responsabilidad del Grupo Planeación y Sistemas por ello se transfiere al responsable Dirección de Información y Tecnología.

Cuadro 6: Análisis de tratamiento de riesgos en PR03.PE01

Etiquetas de fila	CODIGO ESCENARIO	CONTROL ASOCIADO	JUSTIFICACION TRATAMIENTO
	66_PlaF-015	Contrato con Unión Temporal.	El control existe y funciona bien pero no es responsabilidad del Grupo Planeación y Sistemas por ello se transfiere al responsable Dirección de Información y Tecnología.
TRANSFERIR	**66_PlaF-016**	Contrato con Unión Temporal.	El control existe y funciona bien pero no es responsabilidad del Grupo Planeación y Sistemas por ello se transfiere al responsable Dirección de Información y Tecnología.
	66_PlaF-017	Contrato de soporte plataforma voz IP	El control existe y funciona bien pero no es responsabilidad del Grupo Planeación y Sistemas por ello se transfiere al responsable Dirección de Información y Tecnología.

El grupo SGSI determina que con la proyección de estrategias, el riesgo residual estará en niveles tolerables por la organización, por lo tanto autoriza continuar con las siguientes fases del proceso.

El comité define que no se analizarán ni se pondrán en marcha los siguientes componentes de la guía en esta etapa ya que se pronostica un conflicto en la operación interna de la entidad en el nivel regional y es posible generar confusión a los diferentes grupos de la zona debido a las actividades propias del sistema integrado de gestión:

- Definir indicadores para medir la eficiencia de los controles y metas a cumplir.

- Diseñar y realizar pruebas controladas a las salvaguardas para comprobar su rendimiento de forma preventiva.

- Diseñar registro de control al desempeño de los controles implantados.

- Recopilar y analizar los resultados parciales y/o finales de los indicadores de rendimiento de todos los controles.

ETAPA III: Medición de eficacia de los controles.

1. Requisito

El comité de gestión validó que la fase Planeación del Tratamiento del Riesgo está cumplida satisfactoriamente y ha sido documentada. Esto a pesar de no incluir la

definición de indicadores de desempeño de los controles, diseño y ejecución de pruebas a los mismos, los registros y análisis de resultados necesarios debido a razones propias de la organización ya expuestas, pero considera que la metodología es adecuada para cumplir el objetivo de la fase en otro escenario de prueba piloto. Al estar presentes todos los involucrados en el proceso de gestión del riesgo se da por cumplida la comunicación del riesgo para este componente.

2. Acción.

2.1 Validación para que el plan de tratamiento del riesgo sea satisfactorio y aceptado.

En análisis del comité SGSI, se establece que este componente de la guía no puede ser valorado debido a que incorpora la ejecución de actividades que sí se han proyectado a lo largo de la prueba piloto pero no serán realizadas debido a razones propias de la organización ya expuestas. Otro factor es que los requisitos de esta etapa no se cumplieron completamente y por lo tanto harán falta insumos importantes para medir resultados sobre el tratamiento del riesgo. Finalmente el alcance de la prueba piloto en esta instancia se ubica en la fase Planear-Hacer, no en el Hacer.

Por lo anterior no es posible determinar:

- Cuáles riesgos tratados se han reducido a niveles aceptables y cumplen las expectativas de seguridad de las partes interesadas.

- Si es necesario redefinir criterios o fases del ciclo de gestión del riesgo.

- Si se deben aceptar riesgos sin tratamiento o tratados pero por encima de los niveles aceptables para la organización, justificados por beneficios indirectos o costos de procesamiento demasiado altos.

Etapa IV: Seguimiento, revisión y valoración periódica de riesgos.

1. Requisito

El comité SGSI determina que no hay información suficiente para cumplir esta etapa de la guía ya que la fase tratamiento del riesgo ha sido cumplida hasta su

fase Planear-Hacer, aplicando el mismo soporte dado en la etapa III. Sin embargo, el comité nuevamente considera que la metodología es adecuada para cumplir el objetivo de la fase en otro escenario de prueba piloto.

2. Acción

2.1 Comunicar el riesgo.

El grupo SGSI establece que a lo largo de la planeación del proceso de gestión del riesgo se han realizado varios comités donde han participado los líderes de áreas involucradas en el proceso bajo análisis en la prueba piloto, donde se han tomado las decisiones de alto nivel objeto del diseño del proceso. Para el caso del grupo Planeación y Sistemas Regional Risaralda, las áreas mencionadas son Grupo de Sistemas, Grupo EPICO y Grupo de apoyo financiero conformados únicamente por los profesionales respectivos quienes a su vez conforman el grupo SGSI como se determinó en la acción Organización de la Seguridad. Por lo tanto, esta acción ha sido cumplida satisfactoriamente hasta la fase Planear del proceso de gestión del riesgo, pero no podrá ser cumplida en adelante porque no se ejecutará la fase Hacer en esta prueba piloto por las razones mencionadas en las etapas anteriores.

2.2 Monitoreo y revisión del riesgo.

El comité estipula que es otra acción de la guía dependiente de la ejecución del proceso de gestión del riesgo y por lo tanto tampoco será posible cumplirla en este escenario de la prueba piloto por los motivos ya conocidos, aunque se pronostica una metodología válida para otros casos. Es decir que en esta instancia no hay alcance e insumos para documentar tareas de supervisión del riesgo ni redefiniciones del ciclo de gestión ya que sus resultados son producto de tareas que no se practicarán, como: esperar resultados al final del periodo de análisis definido de seis (6) meses, ante un incidente o evento de seguridad, cambios en el mapa de procesos de la organización, modificación de los requisitos de seguridad, reformas en el organigrama de la organización, cambios en la asignación presupuestal para la gestión e indicadores de eficiencia de controles implantados, etc.

3. Resultados

3.1 ETAPA I: Identificación y Evaluación para el Tratamiento de los Riesgos.

- Compromiso de la alta dirección mediante documento de aprobación para aplicar la guía de gestión del riesgo al procedimiento *PR15-MPA6 Manejo de Medios Removibles v1* en el Grupo Planeación y Sistemas Regional Risaralda, particularmente al área de Apoyo Financiero en el procedimiento *PR03.PE01 Procedimiento de Seguimiento Metas Sociales y Financieras v1.*

- Informe Diagnóstico Inicial del SGSI en la Organización.

- Acta de reunión del comité del grupo Planeación y Sistemas Regional Risaralda donde se declara y socializa el apoyo a la prueba piloto para gestionar el riesgo, se define la organización de la seguridad para tal fin y las acciones sobre el plan de continuidad del negocio.

- Acuerdos de confidencialidad con la entidad firmados por los ejecutores de la prueba piloto.

- Plan de comunicación, sensibilización y divulgación hacia la organización.

- Acta de reunión del Comité de Gestión donde se establecen los requisitos de seguridad para al área de Apoyo Financiero en la Regional Risaralda y definir presupuesto para la aplicación del proceso de gestión del riesgo. También se incluye el análisis, estimación y valoración de riesgos donde se prioriza la atención a los activos.

3.2 ETAPA II: Selección de objetivos de control y controles.

- Acta de reunión del Comité de Gestión donde se evidencia el cumplimiento satisfactorio del requisito previo: valoración de riesgos. Hace parte de la documentación de resultados, la consolidación de objetivos de control y controles formalizados en la declaración de aplicabilidad aprobada por la alta dirección y su reconocimiento para enfrentar los riegos con la disponibilidad y profundidad requerida por la organización. También hace parte de la documentación de resultados, la designación de responsables de la

aplicación de las salvaguardas seleccionadas, el plan definitivo para tratar los riesgos proyectado para llevarlos a los niveles aceptables, los insumos para monitorear y revisar el proceso y finalmente la socialización hacia las partes interesadas como parte de la fase Comunicar el Riesgo.

3.3 ETAPA III: Medición de eficacia de los controles.

- Acta de reunión del Comité de Gestión demostrando el cumplimiento satisfactorio del requisito previo: fase Tratamiento del Riesgo. De igual forma la documentación y aceptación de los resultados y acciones tomadas luego de la ejecución del plan para enfrentar los escenarios incidentes y soportada en la fase monitoreo y revisión del riesgo, discriminando los riesgos en niveles aceptables y los intolerables pero con tratamiento de manera estratégica para la organización. Por último, la socialización hacia las partes interesadas como parte de la fase Comunicar el Riesgo.

3.4 Etapa IV: Seguimiento, revisión y valoración periódica de riesgos.

- Acta de reunión del Comité de Gestión donde se evidencia cumplimiento satisfactorio del requisito previo: fase Tratamiento del Riesgo. Además ante el resultado de este plan, deben incluirse las evidencias sobre las tareas de supervisión del riesgo, análisis de resultados y planes de acciones motivadas por las variables que disparan esta acción de forma permanente a lo largo del ciclo de gestión. Por último la socialización hacia las partes interesadas por medio de los comités primarios y secundarios como parte de la fase Comunicar el Riesgo.

ANEXO C
MODELAMIENTO DE PROCESOS EN BIZAGI

BUSSINESS PROCESS MANAGEMENT - BPM: La Administración de Procesos de Negocio es una metodología corporativa cuyo objetivo es mejorar el desempeño (Eficiencia y Eficacia) de la Organización a través de la gestión de los procesos de negocio que se deben diseñar, modelar, organizar, documentar y optimizar de forma continua.

Un proceso de negocio representa una serie discreta de actividades o tareas que pueden incluir personas, aplicativos, eventos de negocio y organizaciones. Las ventajas del modelado BPM es el entendimiento, visibilidad y control de los procesos de negocio de una organización. Para soportar esta estrategia es necesario contar con un conjunto de herramientas que den el soporte necesario para cumplir con el ciclo de vida de BPM, estas herramientas normalmente siguen una notación común denominada BPMN (Business Process Modeling Notation).[30]

BUSINESS PROCESS MODELING NOTATION – BPMN: La Notación para el Modelado de Procesos de Negocio es una notación gráfica estandarizada que permite el modelado de procesos de negocio en un formato de flujo de trabajo (workflow). El principal objetivo de BPMN es proporcionar una notación estándar que sea fácilmente legible y entendible por parte de todos los involucrados e interesados del negocio.

BPMN tiene la finalidad de servir como lenguaje común para cerrar la brecha de comunicación que frecuentemente se presenta entre el diseño de los procesos de negocio y su implementación.[31]

BIZAGI: Es una compañía privada establecida en 1989 en Inglaterra, cuyo objetivo es la provisión de soluciones para la automatización de procesos de

[30] Tomado de: http://es.wikipedia.org/wiki/Gesti%C3%B3n_de_procesos_de_negocio [En línea] Consultado 15/02/2014.
[31] Tomado de http://es.wikipedia.org/wiki/Business_Process_Modeling_Notation [En línea] Consultado 15/02/2014

negocio a través de una suite ofimática compuesta por un Modelador de Procesos (Bizagi Process Modeler) y una suite de BPM (Bizagi BPM Suite).

El Modelador de Procesos es utilizado para diagramar, documentar y simular procesos de manera gráfica usando la notación estándar BPMN.

La Suite consiste de dos herramientas: Bizagi Studio, el módulo de construcción, y Bizagi BPM Server para ejecución y control. En Bizagi Studio el usuario define el modelo asociado al proceso de negocio (flujograma, reglas de negocio, interfaz de usuario, etc) para la ejecución del mismo. Los modelos se guardan en una base de datos y son utilizados posteriormente en la ejecución por Bizagi BPM Server. Bizagi BPM Server ejecuta un Portal de Trabajo para los usuarios finales en un PC o cualquier dispositivo móvil.[32]

Dentro del alcance de este proyecto, se realizó todo el modelamiento de los procesos de Gestión del Riesgo descritos en el documento base utilizando el Modelador de Procesos de Bizagi, dejando de esta manera la puerta abierta para la implementación y programación de los modelos propuestos y finalmente para la ejecución de los módulos que se construyan como parte del alcance de otro proyecto que guarde relación con la implementación de la norma ISO/IEC 27001.

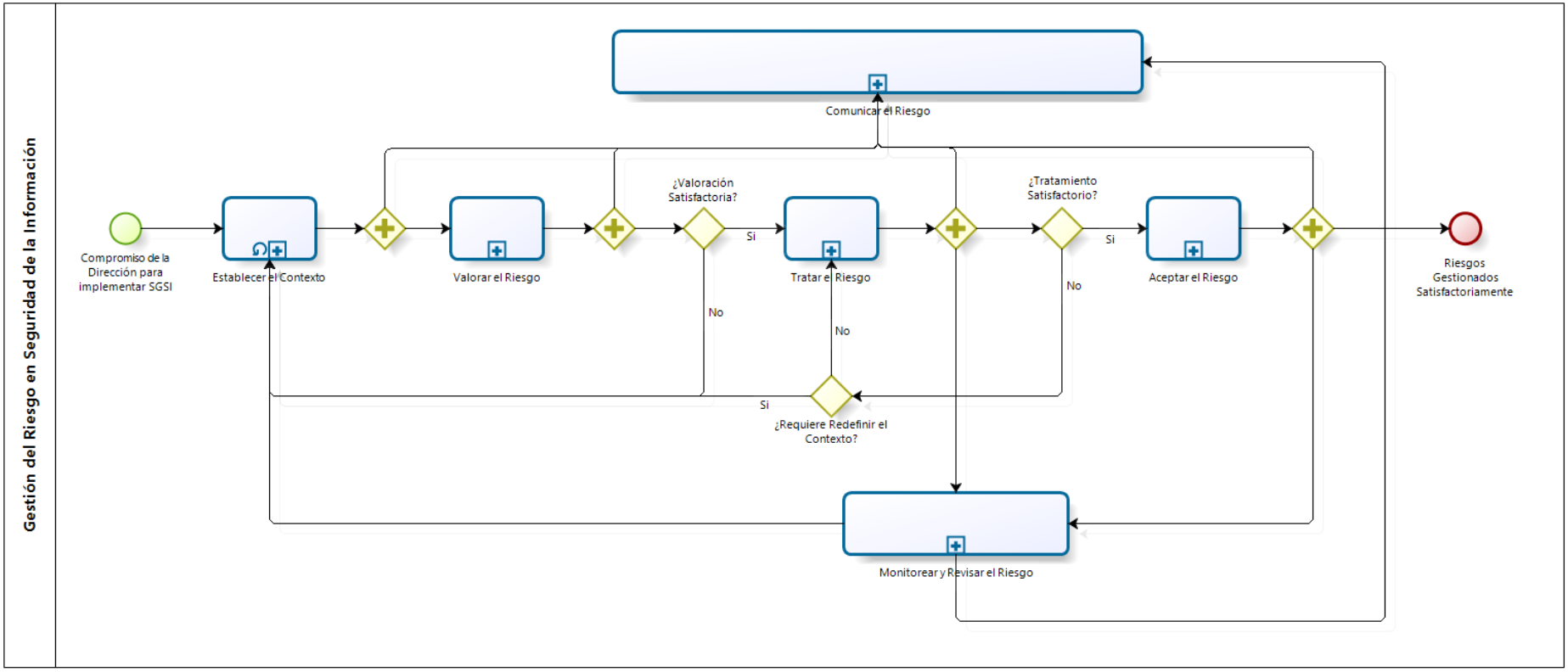
MODELAMIENTO DE PROCESOS DE GESTIÓN DEL RIESGO

Utilizando la notación BPM a través del Modelador de Procesos de Bizagi, se ha modelado todo el proceso de Gestión del Riesgo siguiendo el flujo de tareas descrito en la figura 1 de la *Guía para Gestionar el Riesgo y Seleccionar Controles en la Implementación del SGSI*. De esta manera, se partió modelando el diagrama general de la Gestión del Riesgo y se fue recorriendo cada actividad subsiguiente correspondiente a los numerales de la norma ISO/IEC 27005.

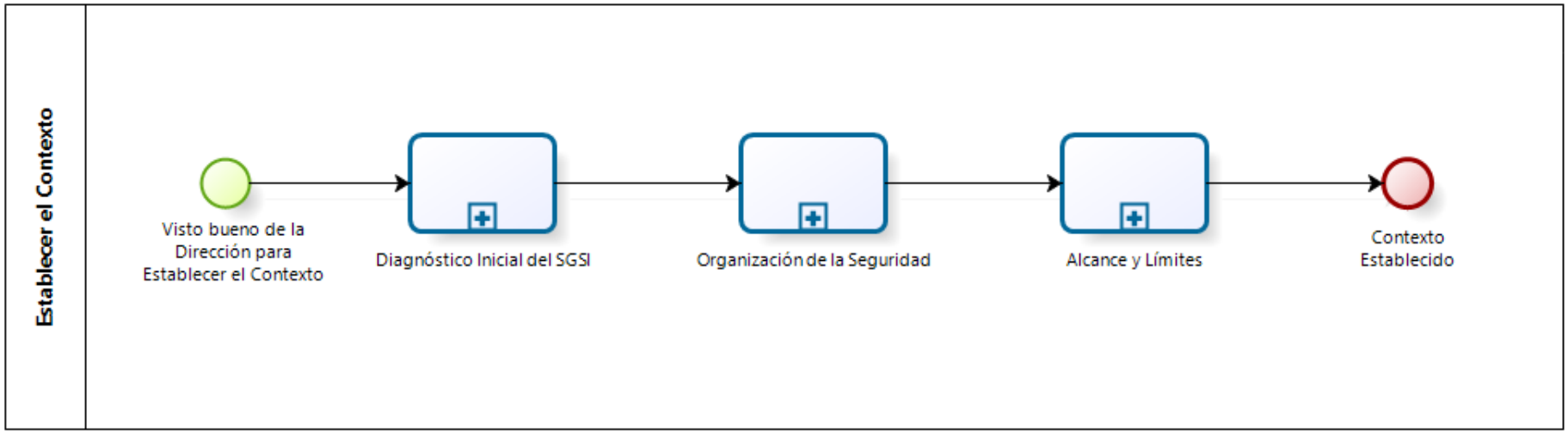
La notación BPMN ofrece la posibilidad de modelar procesos dentro de otros procesos, lo que permitió diagramar con mayor detalle las actividades que corresponden a cada uno de los numerales de la norma pudiendo identificar gráficamente cada parte del proceso de Gestión del Riesgo.

[32] Tomado de http://es.wikipedia.org/wiki/Bizagi [En línea] Consultado 15/02/2014

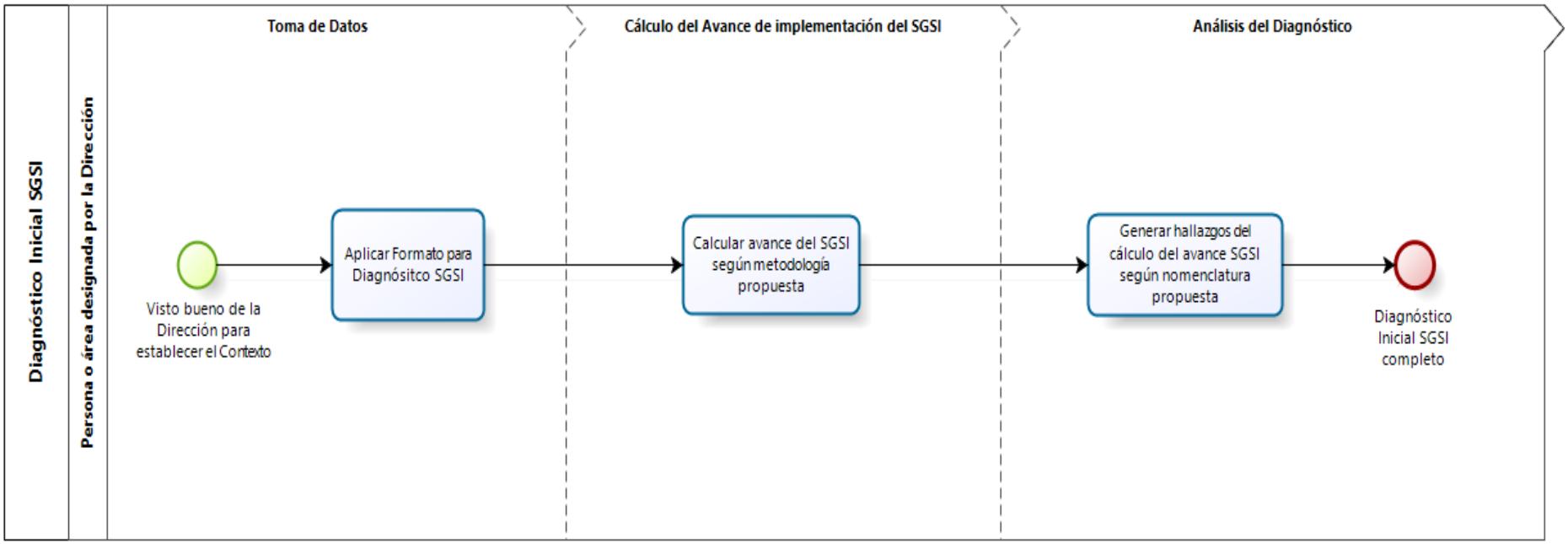
Diagrama general del proceso de Gestión del Riesgo – Norma ISO/IEC 27005.



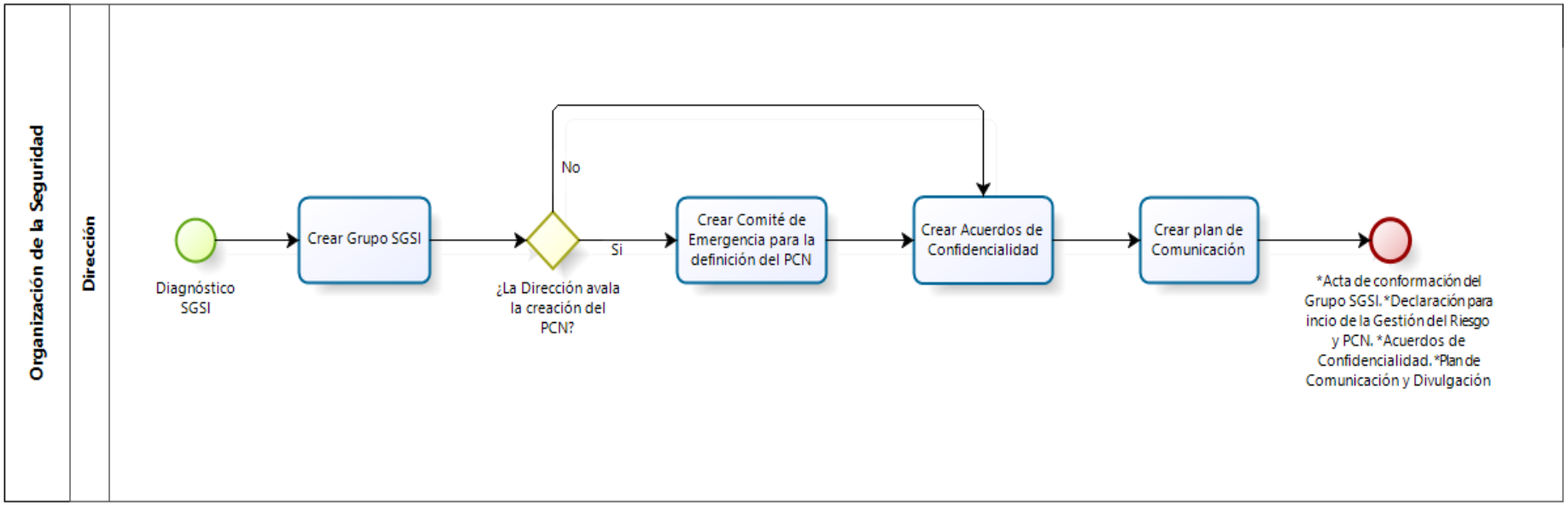
1. Fase Establecer el Contexto.



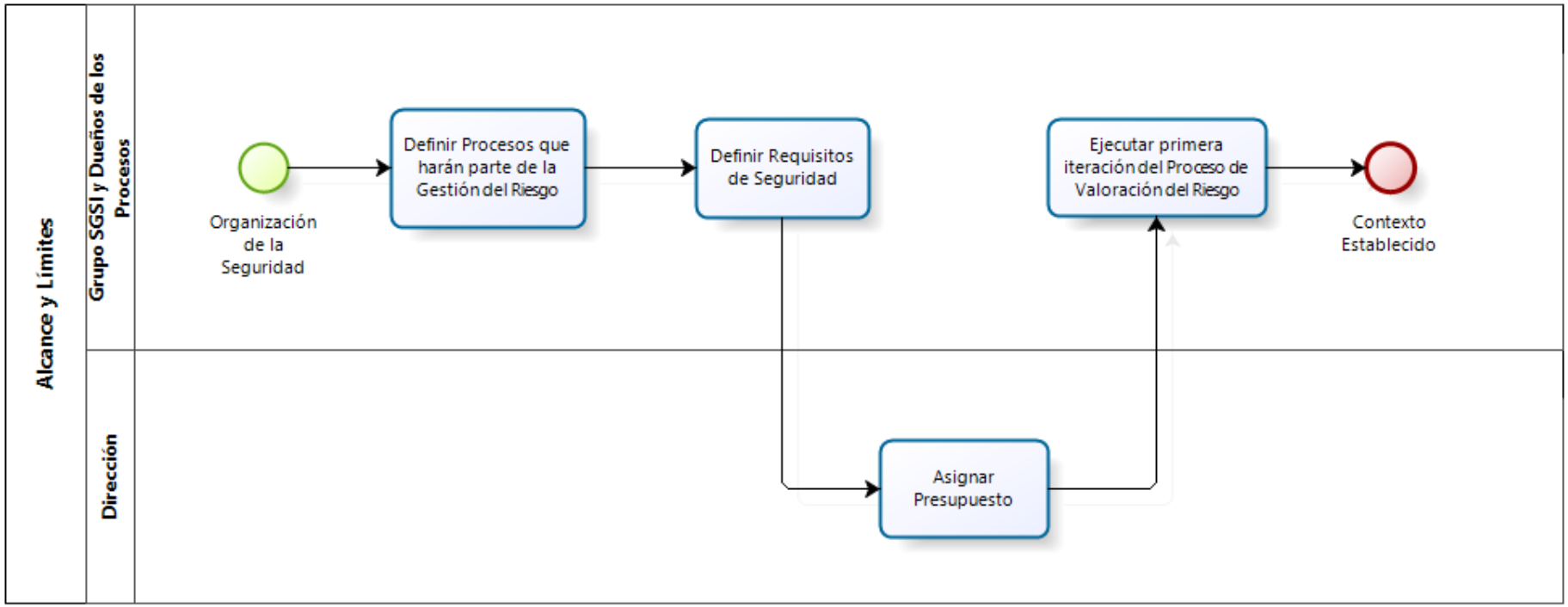
1.1. Subfase Diagnóstico inicial del SGSI.



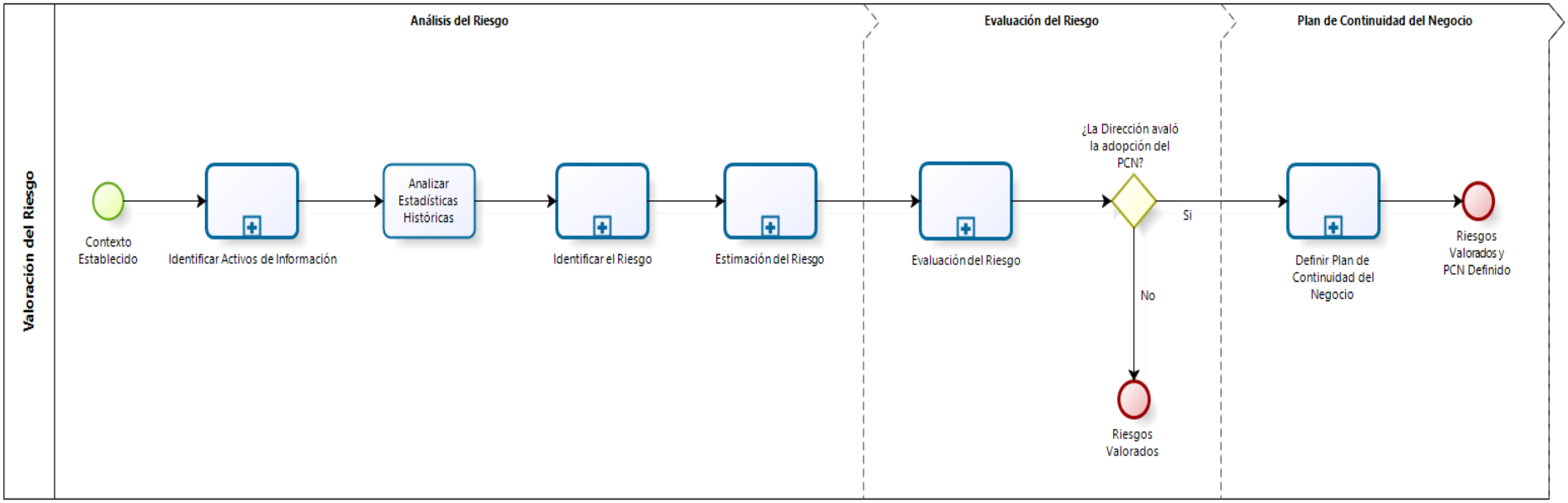
1.2. Subfase Organización de la Seguridad.



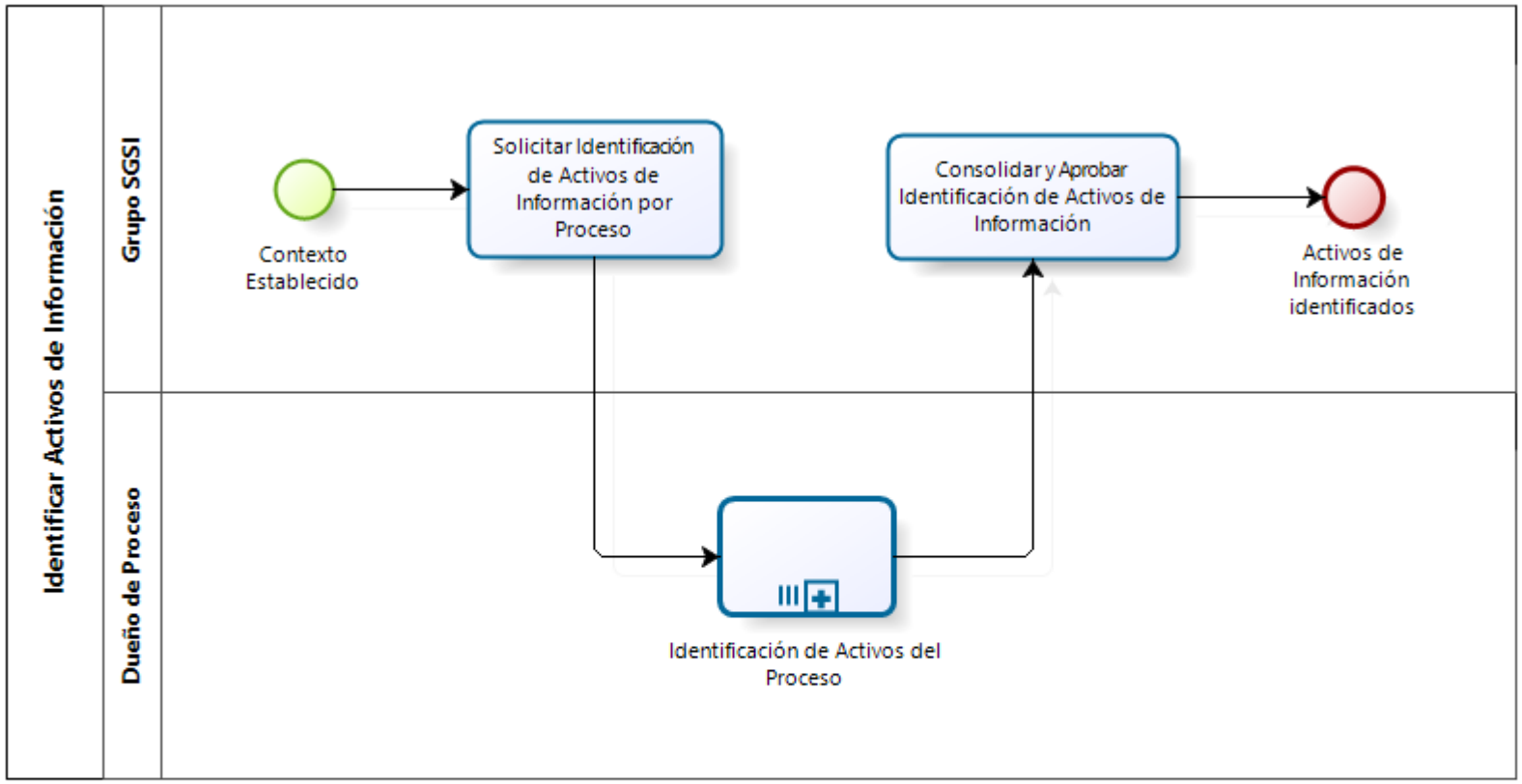
1.3. Subfase Alcance y Límites.



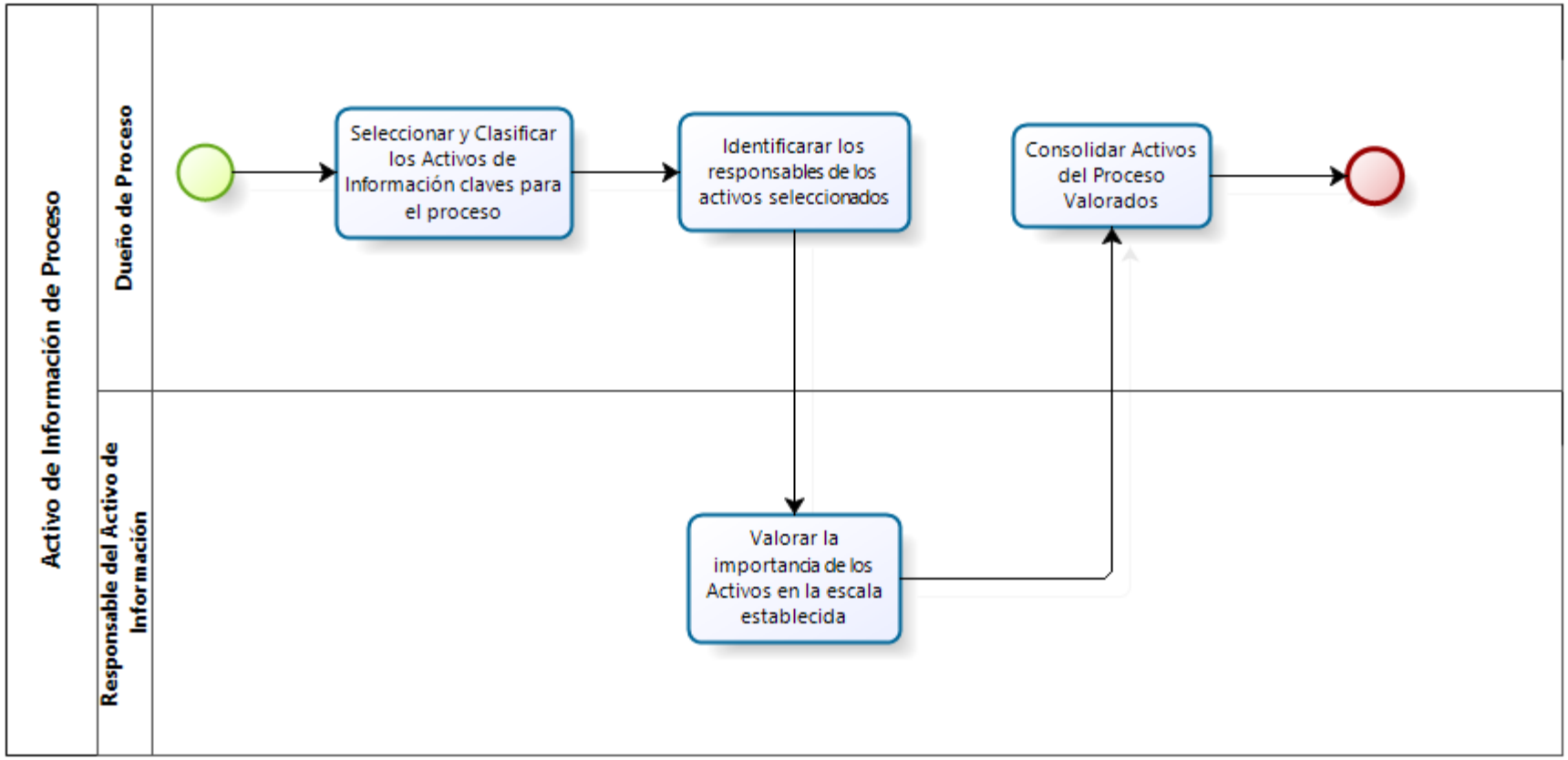
2. Fase Valoración del Riesgo (Análisis + Evaluación del Riesgo).



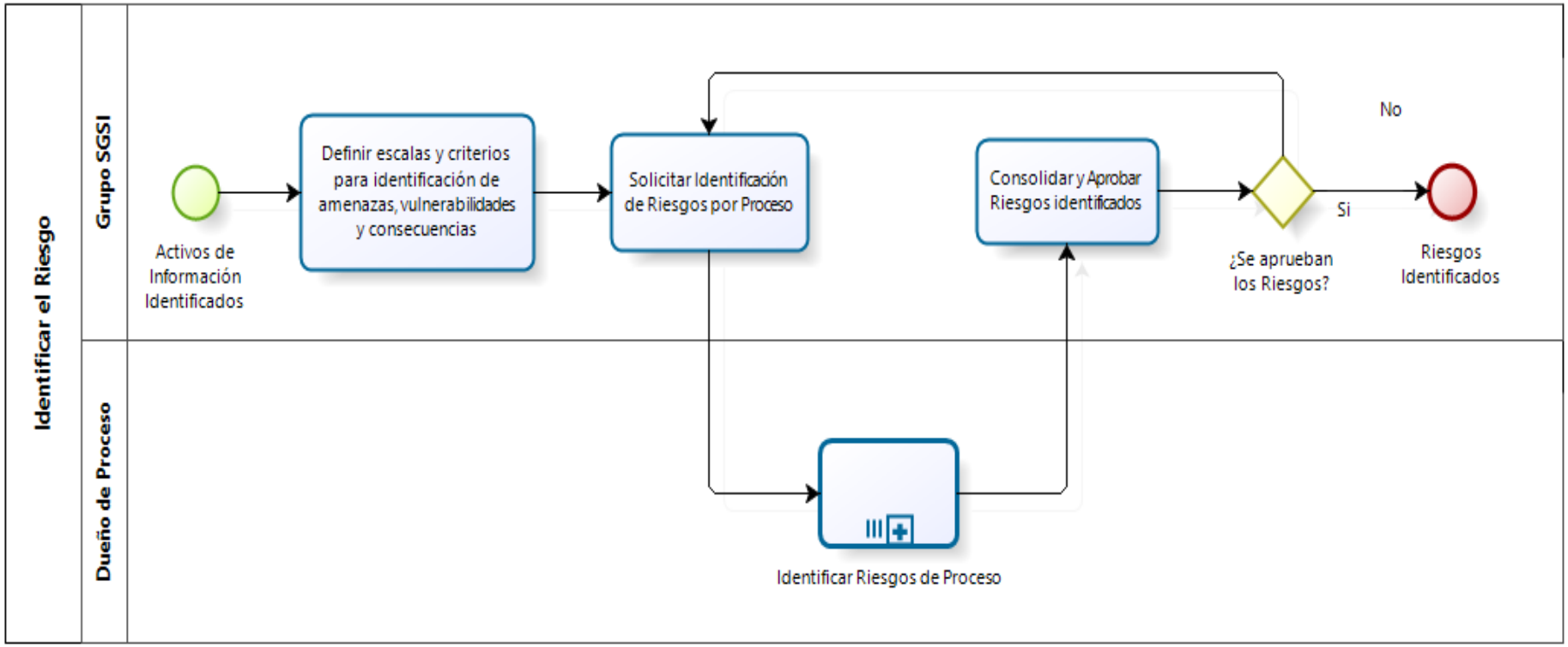
2.1. Fase Análisis del Riesgo – Identificación de Activos de Información.



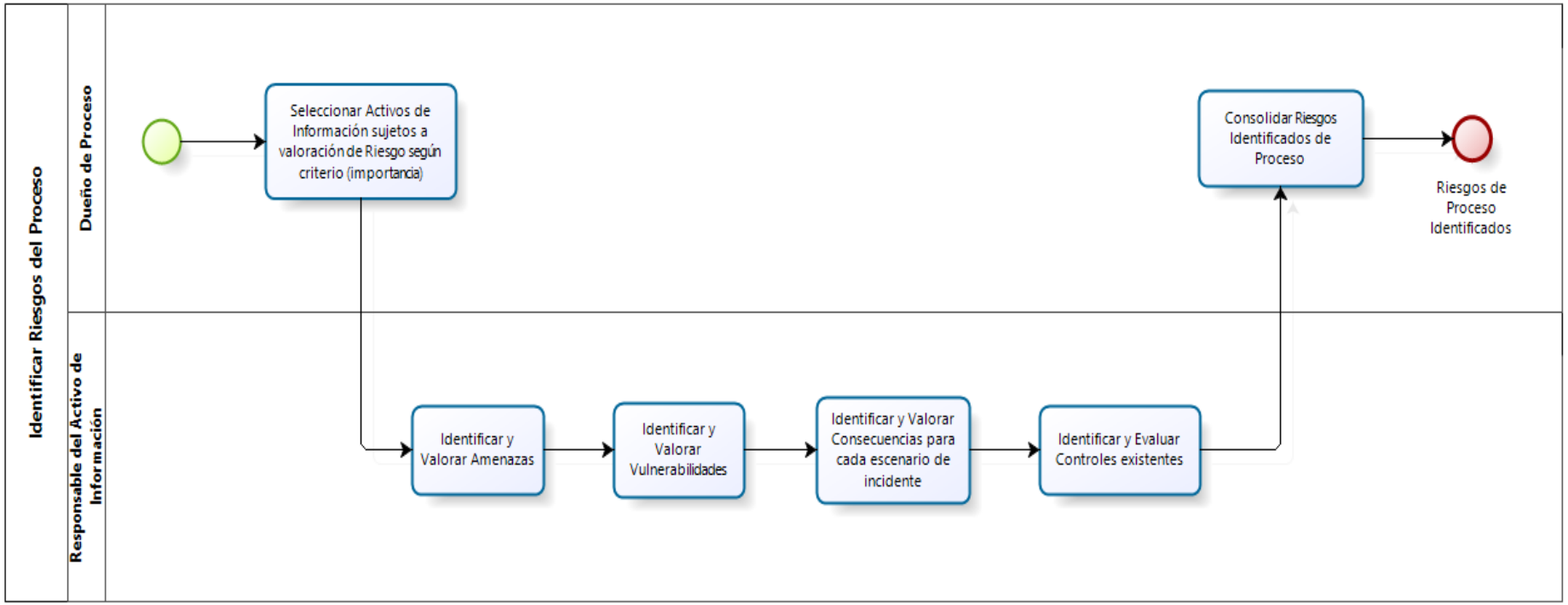
2.1.1. Subfase Identificación de Activos de Información del Proceso.



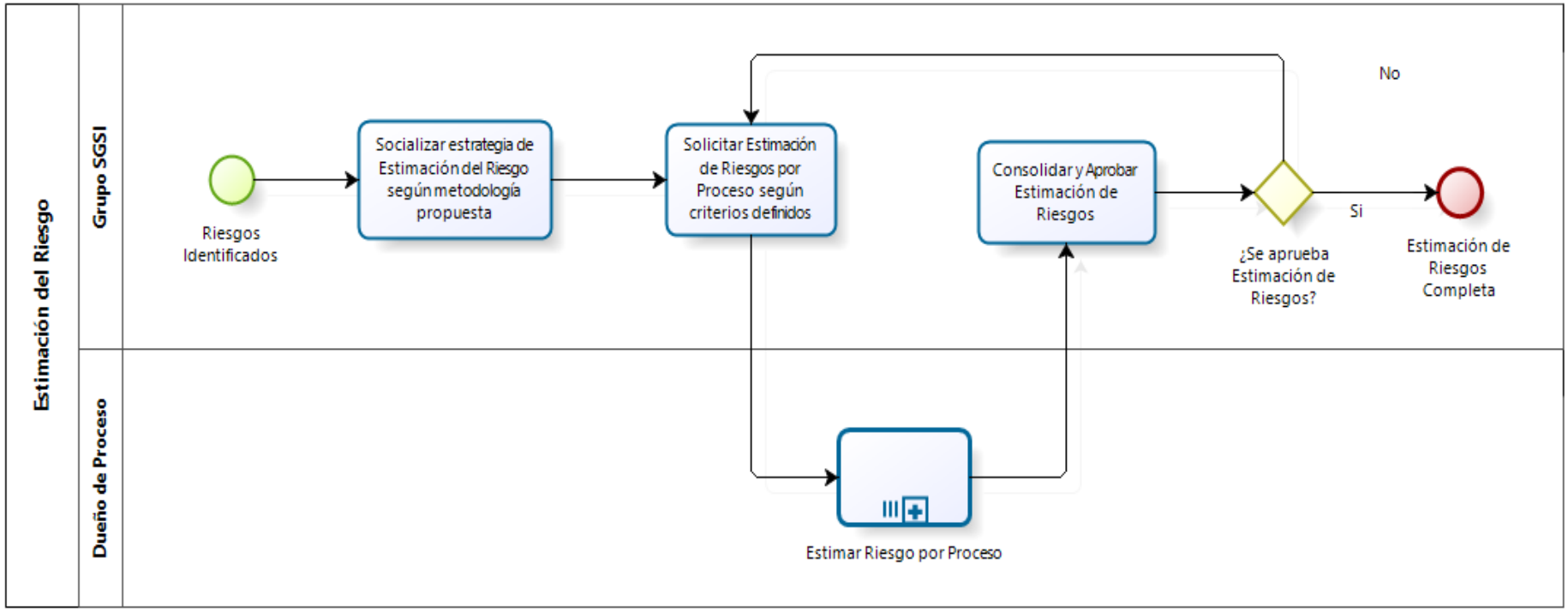
2.2. Fase Análisis del Riesgo – Identificación de Riesgos.



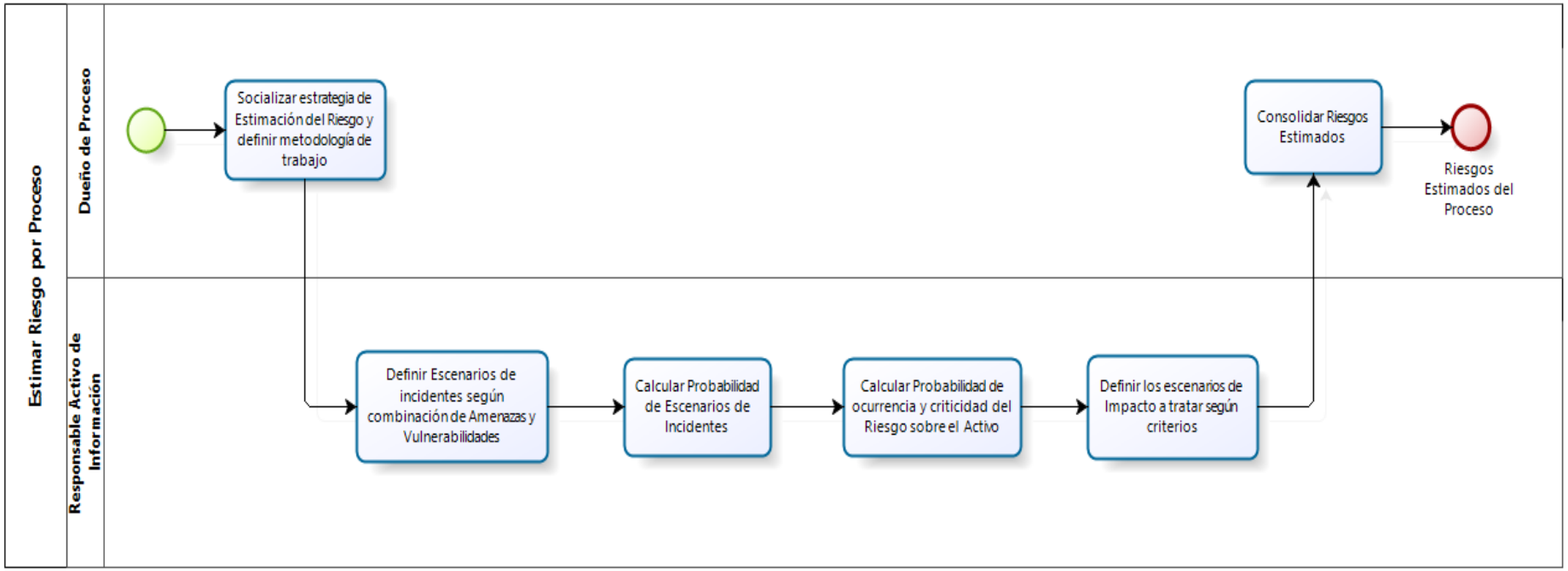
2.2.1. Subfase Identificación de Riesgos por Proceso.



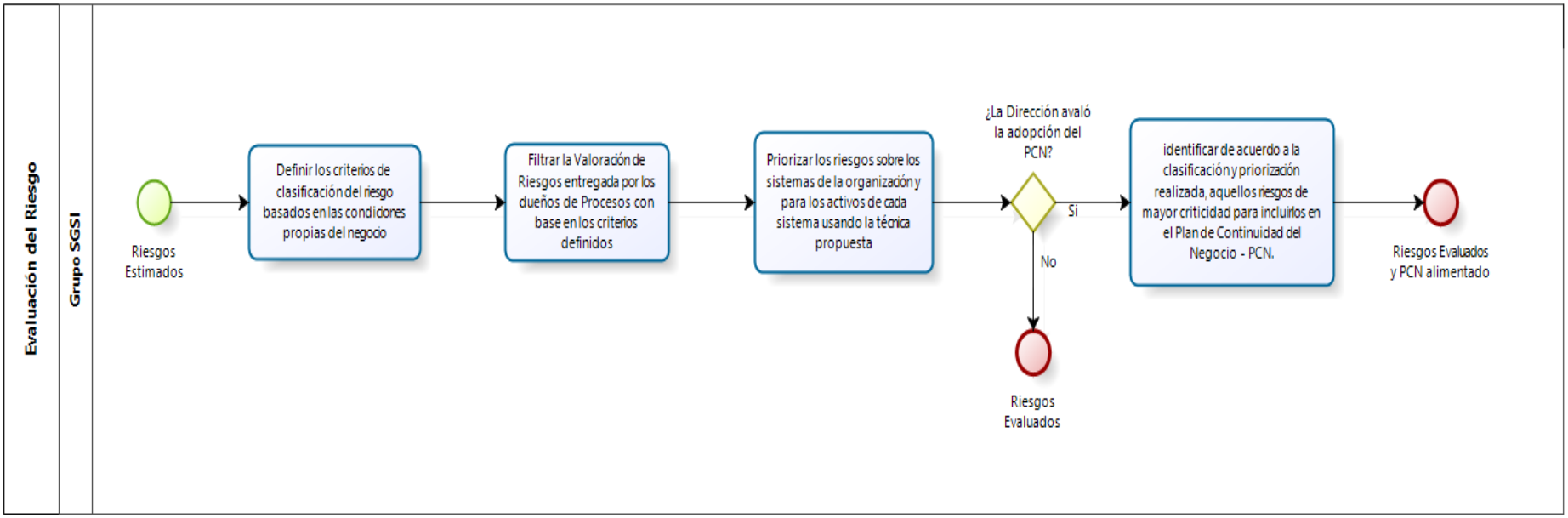
2.3. Fase Análisis del Riesgo – Estimación de Riesgos.



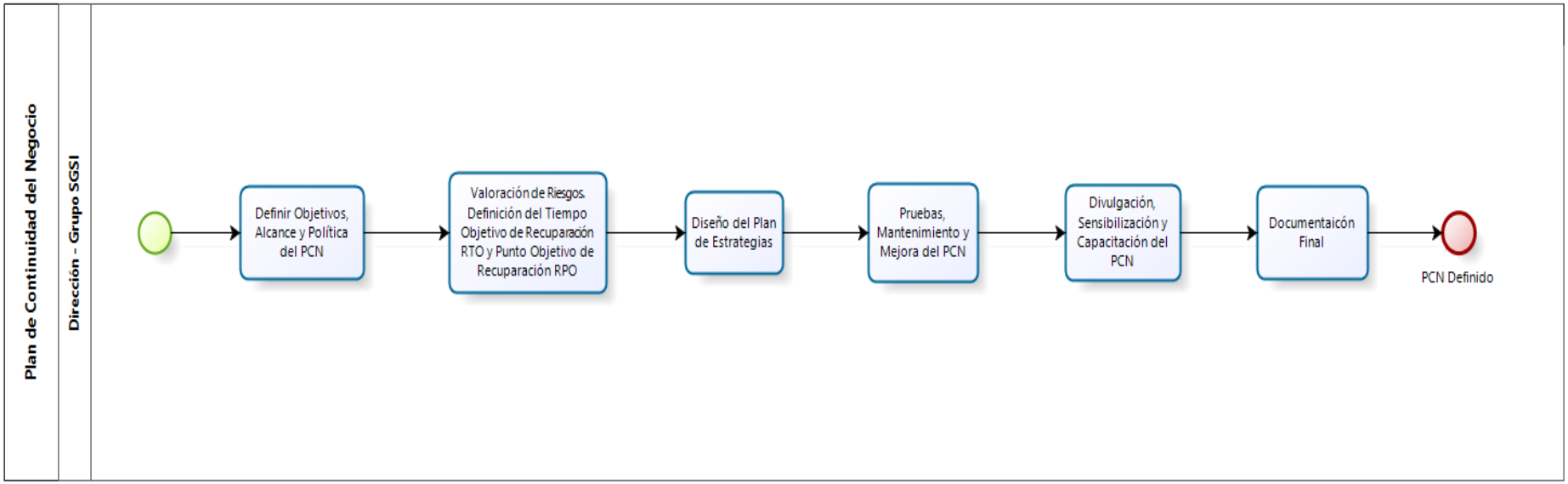
2.3.1. Subfase Estimación de Riesgos por Proceso.



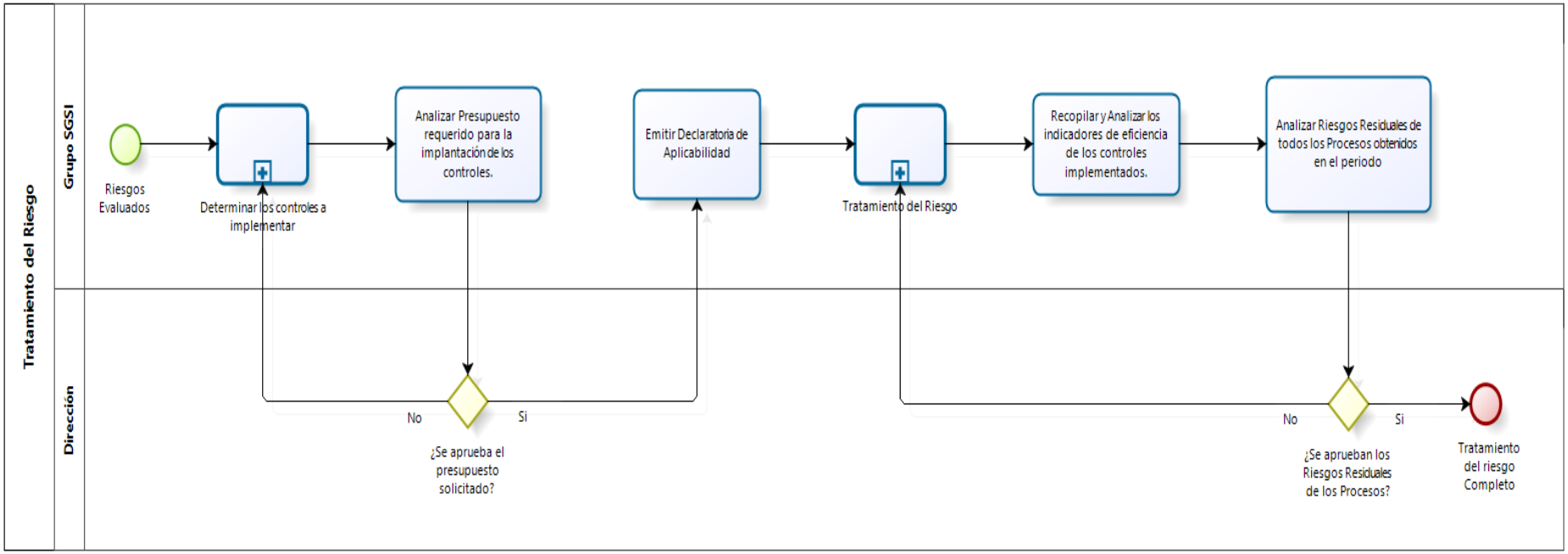
2.4. Fase Evaluación del Riesgo.



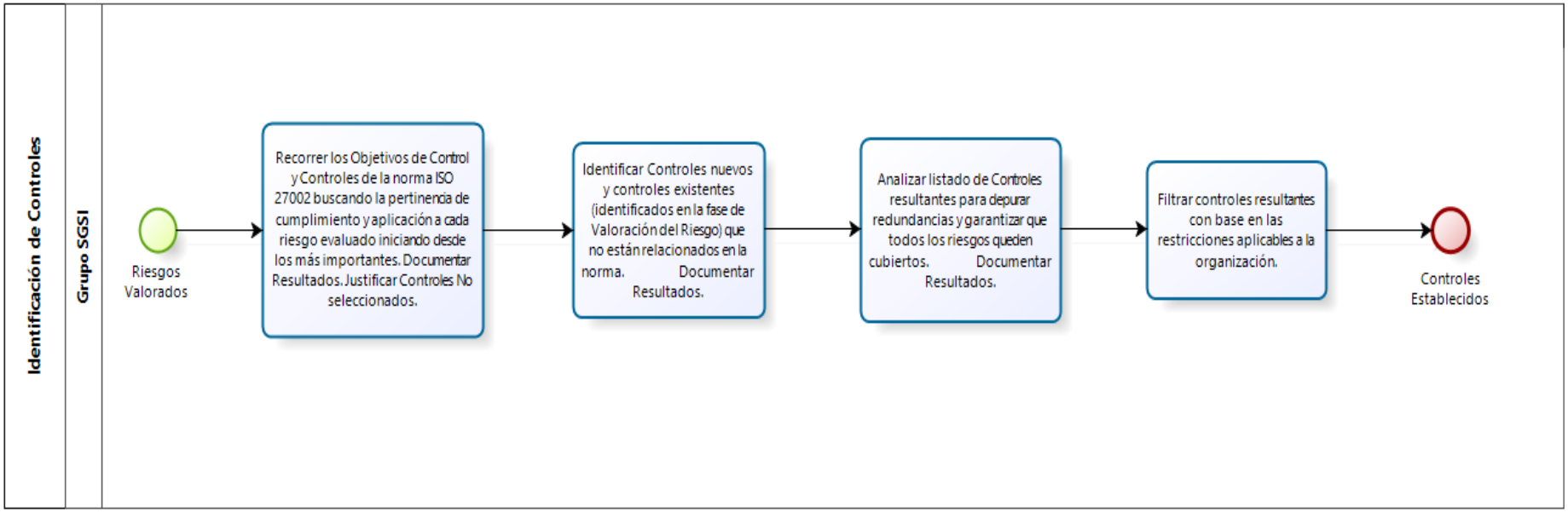
2.5. Fase Establecimiento del Plan de Continuidad del Negocio.



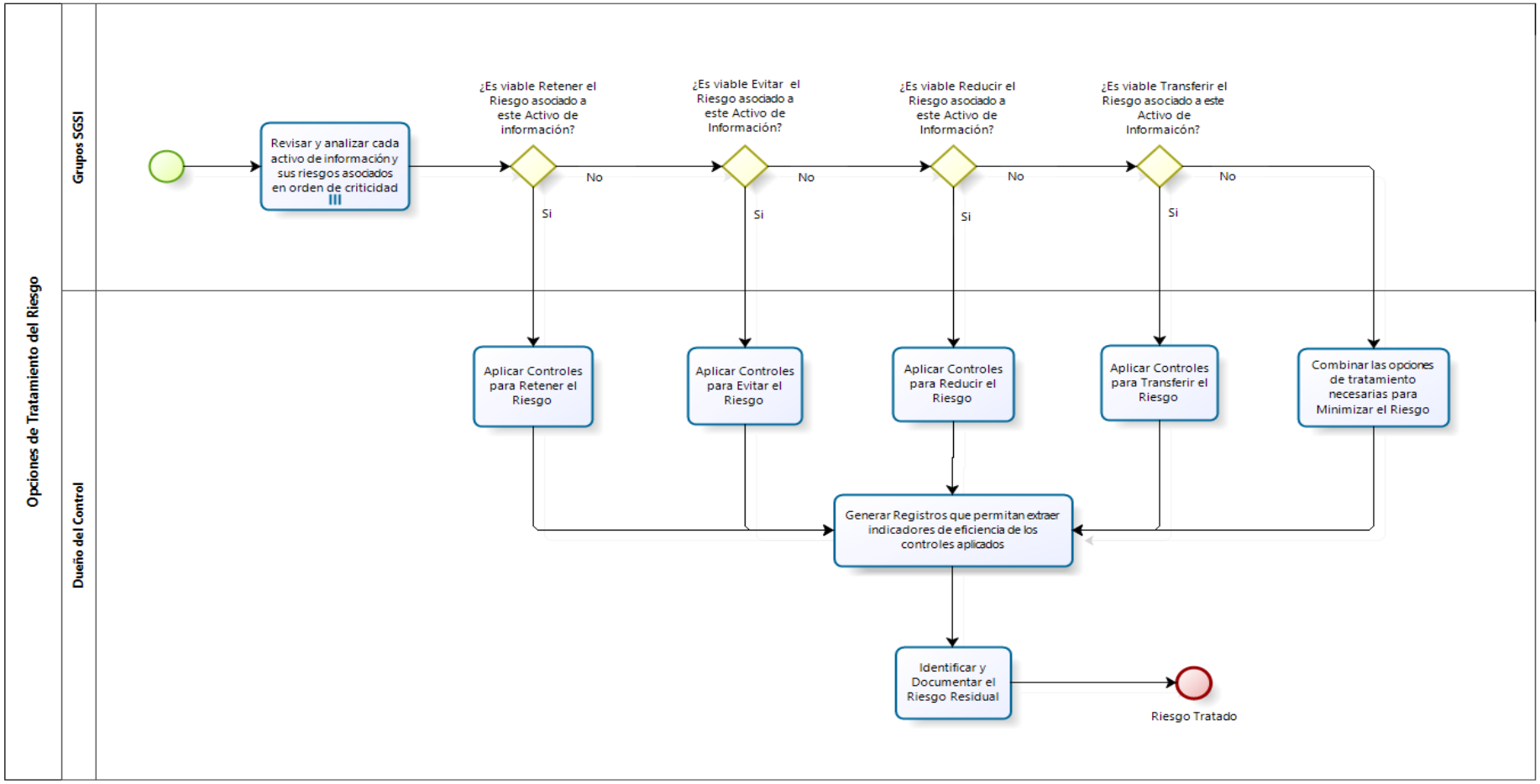
3. Fase Tratamiento del Riesgo.



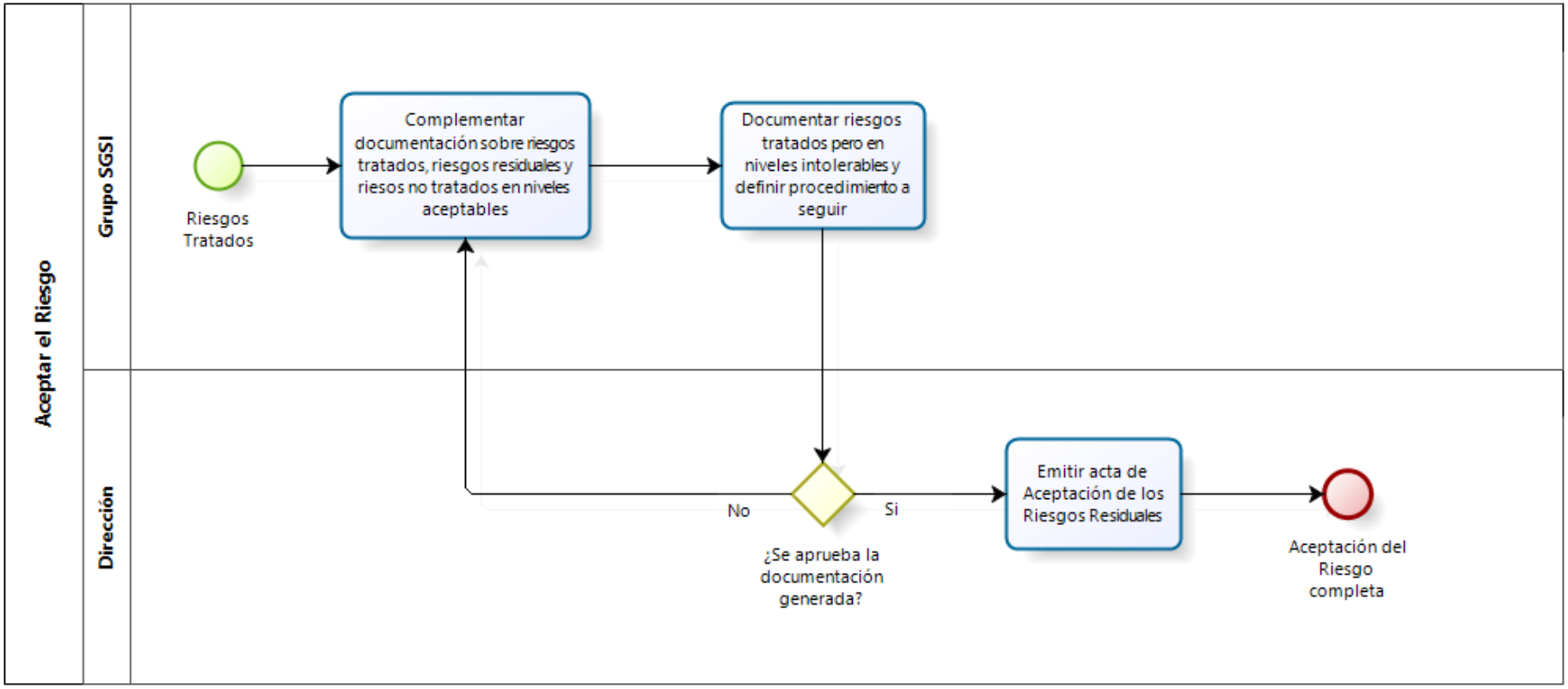
3.1. Subfase Identificación de Controles.



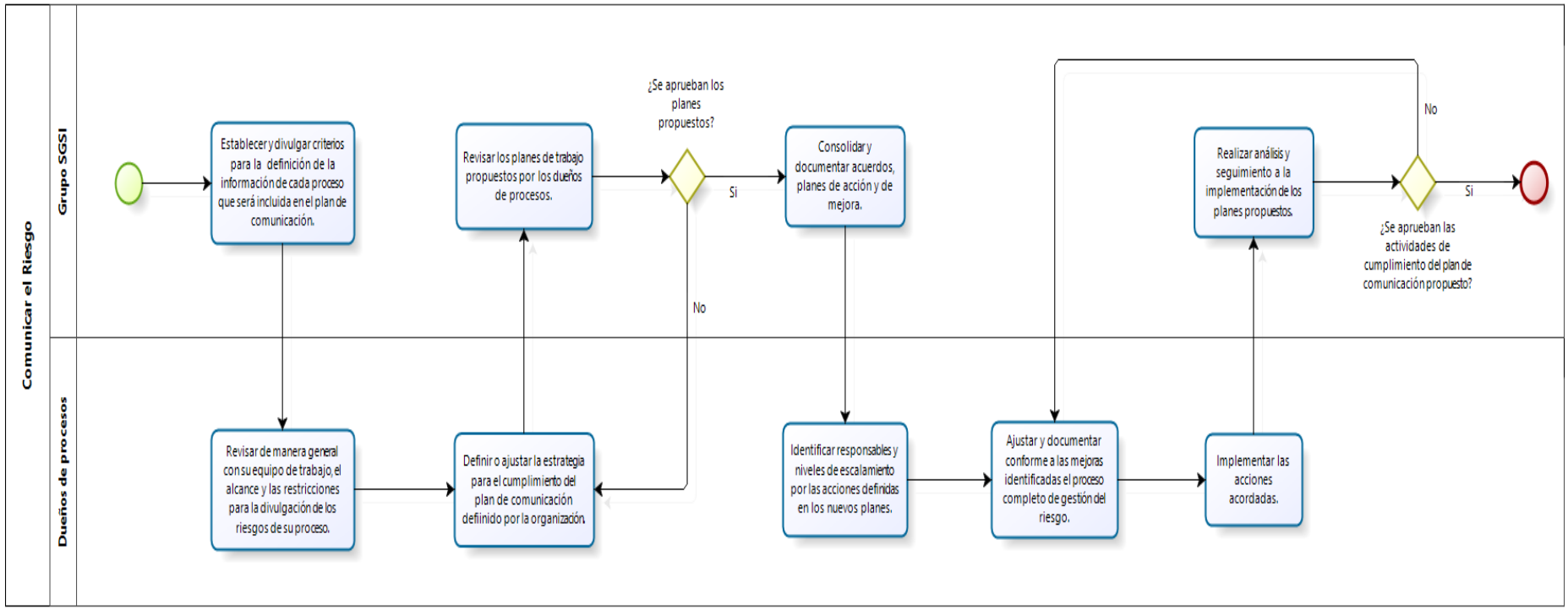
3.2. Subfase Opciones para el Tratamiento del Riesgo.



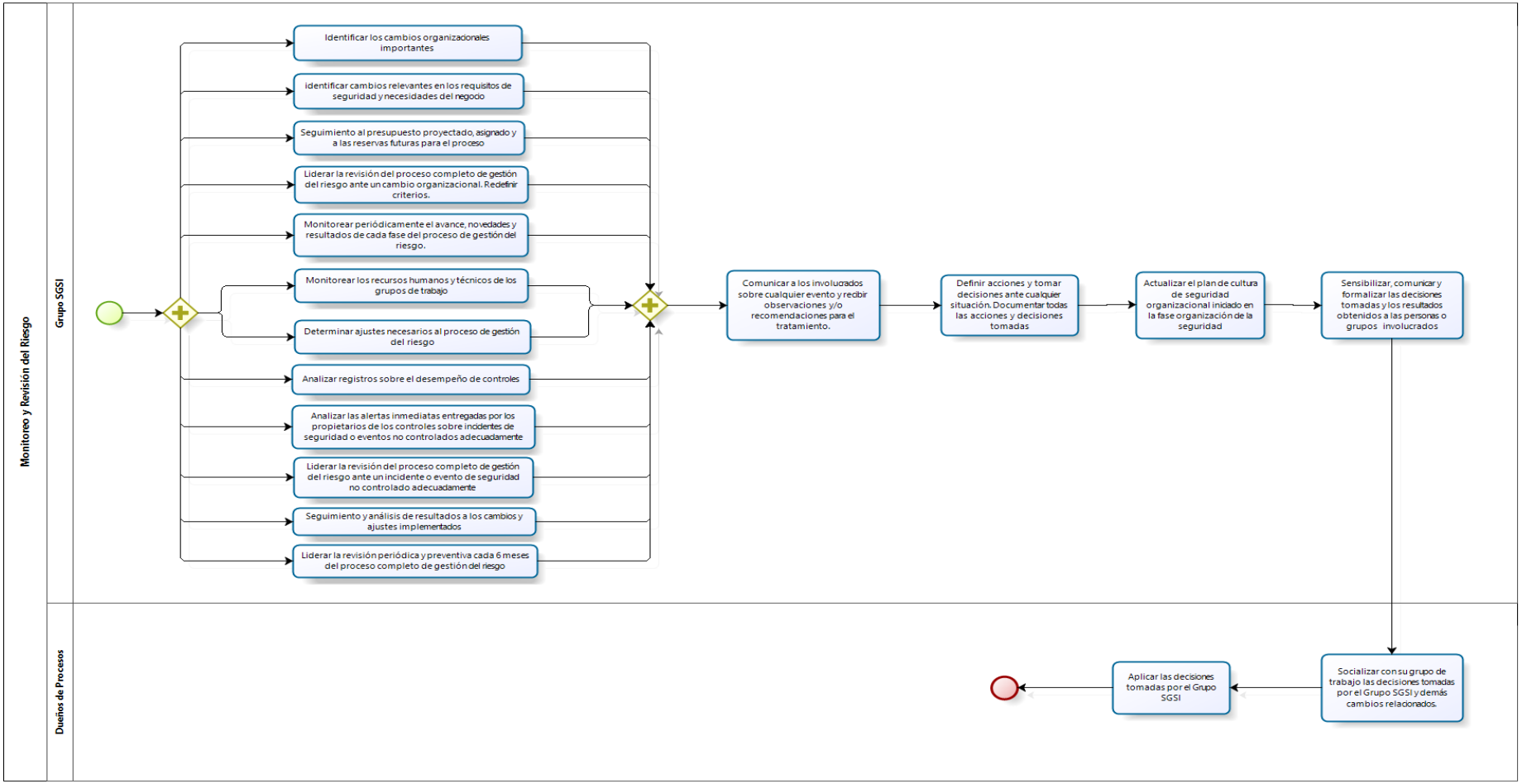
4. Fase Aceptar el Riesgo.



5. Fase Comunicación del Riesgo.



6. Fase Monitoreo y Revisión del Riesgo. P1.



GUÍA BASADA EN EL GRUPO DE NORMAS INTERNACIONALES ISO/IEC 27000 PARA GESTIONAR EL RIESGO Y SELECCIONAR CONTROLES EN LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

ING. ELKIN REINA GARCÍA
ING. JOSÉ RAÚL MORALES RAMÍREZ

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y CIENCIAS DE LA COMPUTACIÓN
PROGRAMA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
ESPECIALIZACIÓN EN REDES DE DATOS
PEREIRA
2014

CONTENIDO

pág.

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

I. INTRODUCCIÓN

El estándar ISO/IEC 27001 define un Sistema de Gestión de Seguridad de la Información (SGSI) basado en procesos bajo el modelo Planear-Hacer-Verificar-Actuar (P-H-V-A) el cual se utiliza para operar y mantener el sistema. En cada fase se establecen las actividades a realizar con el fin de conformar el sistema dentro de una operación eficiente.

Cualquier organización busca como uno de sus objetivos principales, mantener su negocio en continua operación. Asegurar la información vital se hace necesario e indispensable. Una herramienta de gestión que permite esta labor es implementar un SGSI ya que disminuye los riesgos a los que se someten los activos de información.

Una de las actividades claves es conocer los procesos corporativos e identificar los activos de información, sus características y las dependencias que permiten obtener un producto o servicio propio del negocio, también se debe conocer sus amenazas y enfrentarlas adecuadamente. Así es más fácil organizar los sistemas de información, establecer políticas y/o procedimientos y definir controles que mediante la medición periódica de su eficacia disminuirán los eventos de seguridad. Cuándo existen controles para minimizar o evitar la ocurrencia de un riesgo y este se materializa, se denomina evento. Se llama incidente cuando las consecuencias del riesgo se sufren y no han sido previstas.

Es importante para la alta dirección de la organización y para quienes deben documentar y ejecutar los procesos de implementación del SGSI o solamente para realizar la fase de gestión del riesgo, iniciar con la fase planear definiendo un estado preliminar que indique qué tan preparada se encuentra la organización para afrontar la implantación del nuevo sistema y ayudar así a identificar los recursos que se requieren para comenzar con el proceso. Para esto se debe realizar un completo levantamiento de información que cubra cada uno de los temas exigidos por la norma ISO/IEC 27001 y que además cada punto sea medible tanto cualitativa como cuantitativamente, para que de esta manera se pueda definir cuáles son los procesos que exigen mayor atención de acuerdo a su calificación y para llevar un control sobre el avance general de la implementación del alcance definido en el SGSI o para realizar la gestión del riesgo exclusivamente.

Los incidentes y eventos de seguridad son aquellas amenazas que explotan una vulnerabilidad de un activo de información materializándose en un riesgo. Por lo tanto gestionar el riesgo a través de un SGSI es un proceso cuyo objetivo es mantenerlos en un nivel aceptable para la organización amparando así la confidencialidad, integridad y disponibilidad de los activos de información ante clientes, proveedores, para sí mismo y cualquier parte interesada en el negocio; el resultado final es asegurar los objetivos de rentabilidad del oficio.

Los controles implementados reducirán los riesgos al nivel aceptable, si se producen daños serán de bajo impacto y la continuidad del negocio se asegura. Se deriva de esto un ahorro en los costos que implica prever y racionalizar recursos eliminando inversiones innecesarias o mal diseñadas generando ineficiencia, incumplimiento del marco legal y contractual. Finalmente la Seguridad pasa de ser una serie de actividades organizadas a tener un ciclo de gestión.

Para que el ciclo de gestión funcione adecuadamente, requiere el compromiso y liderazgo de la alta gerencia de la organización debido a su conocimiento y experiencia en el negocio y por su capacidad para implantar nuevos procedimientos en los procesos.

En las compañías donde se esté trabajando para implementar un Sistema Integral de Gestión o que ya se haya implantado por lo menos otro sistema de calidad, se deben ajustar procesos y/o procedimientos ya definidos en su marco operativo, logrando trabajar en paralelo las tareas que involucren todos los sistemas, para evitar reproceso y manteniendo la coherencia entre las actividades de cada sistema.

2. ESTRUCTURA DE LA GUÍA

La guía establece el cumplimiento de actividades enfocadas en cuatro etapas para gestionar el riesgo:

- Identificación y evaluación para el tratamiento de los riesgos.
- Selección de Objetivos de Control y controles.
- Medición de eficacia de los controles.

- Seguimiento: Revisión y Valoración periódica de riesgos.

Cada actividad de la guía establece unos pasos para su cumplimiento:

- Requisitos: Son los datos preliminares y necesarios para cumplir la actividad.

- Acción: Es el objetivo que se busca al desarrollar la actividad, describiendo la forma de realizarla.

- Resultados: Es la información obtenida luego de procesar los requisitos bajo la acción descrita.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

La guía se fundamenta en el conjunto de normas internacionales ISO/IEC 27000 que definen el marco de un Sistema de Seguridad de la Información para gestionar el riesgo. Estas normas han sido diseñadas por ISO, Organización Internacional de Normalización, y por IEC, Comisión Electrotécnica Internacional. Estas entidades son constituidas por los organismos de normalización formales de cada país. En el caso de Colombia es ICONTEC quien nombra las normas como PROYECTO DE NORMA TECNICA COLOMBIANA NTC-ISO/IEC 27000. Para tal fin ISO e IEC han establecido un comité técnico de trabajo llamado ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques[33].

A continuación se hace una descripción de cómo se alinea la guía con cada norma del grupo.

ISO/IEC 27000:2009 presenta un resumen de la familia de estándares, ofrece una introducción a un SGSI, describe el ciclo Planear-Hacer-Verificar-Actuar (P-H-V-A) y presenta términos y definiciones usadas en las normas para precisar términos y evitar confusiones. La guía basa en ella, su fundamento teórico y conceptos.

[33] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO/IEC 27000 2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2009.

El estándar ISO/IEC 27001 es universal para cualquier tipo de compañía, es certificable y auditable, especifica los requerimientos para establecer, implementar, operar, monitorear, y mantener un SGSI basado en procesos bajo el modelo P-H-V-A. El alcance la presente guía es el cumplimiento de la fase Planear y la trata como un subsistema que contiene a su vez un ciclo PHVA, se introduce entonces los conceptos de sub ciclos *Planear-Planear, Planear-Hacer, Planear-Verificar y Planear-Actuar.* Esta norma establece en cada fase las actividades a realizar con el fin de conformar el sistema dentro de una operación eficiente. Incluye un grupo de objetivos de control y controles para la mitigación de los riesgos asociados y están alineados con ISO/IEC 27002. También indica los documentos y registros mínimos que debe contener para evidenciar el grado de funcionamiento del sistema. Aquí básicamente la guía define los criterios y metodología a seguir en sus cuatro etapas orientadas a cumplir los requisitos exigidos. En la fase DIAGNÓSTICO SGSI, la guía establece la forma de analizar el cumplimiento de la fase Planear de la norma frente a lo implementado en la organización, esto es fundamental para establecer la brecha y proyectar acciones orientadas a satisfacer todas las secciones de la norma, especialmente en el Capítulo SGSI, secciones Requisitos Generales, Establecimiento y Gestión. En sus demás capítulos la guía se orienta a modelar los procesos de valoración, tratamiento y monitoreo de riesgos donde se seleccionan controles estableciendo la forma de medir su efectividad, recomendando acciones según corresponda y estableciendo una valoración periódica de todo el proceso, temas tratados en las secciones de Implementación y Operación, Seguimiento y Revisión y Mantenimiento y Mejora del SGSI de la norma.

Respecto a la selección de objetivos de control y controles, la guía se basa en ISO/IEC 27002 ya que dicho estándar expone de manera detallada las buenas prácticas para asegurar los sistemas de información de una organización. Consta de 11 secciones, 39 objetivos de control asociados a cada área, y 133 controles que garantizan el cumplimiento de los objetivos. Para llegar a esta instancia, la guía establece que primero se realiza identificación y estimación de los riesgos, posterior ocurre la valoración, y luego se dan las pautas para su tratamiento. Los controles son seleccionados de esta norma según recomendaciones y criterios de la organización frente a la gestión del riesgo, sin embargo se contempla la incorporación de controles propios diseñados para situaciones particulares o inclusive tomados de otras metodologías. Mediante la declaración de aplicabilidad, requisito obligatorio de ISO/IEC 27001, todos los anteriores son analizados justificando y documentando las razones para su selección o exclusión, es decir,

ninguno queda sin revisión garantizando una completa exploración a posibles incidentes de seguridad.

Los procedimientos, actividades, análisis y resultados planteados en la guía sobre gestión del riesgo en la seguridad de la información son extraídas de ISO/IEC 27005 cuyo objeto de aplicación es proveer pautas y criterios sobre este aspecto. Sin embargo la norma no es una metodología específica, es muy general y corresponde a cada organización definir el enfoque según su naturaleza, eso sí, es aplicable a todo tipo de organización. Esta guía es una de muchas metodologías existentes bajo tal estructura camino a implementar un SGSI, pero recopila buenas prácticas producto de la experiencia de los autores. Esta norma al estar implícita en la guía ofrece continuidad, soporte y cumplimiento a ISO/IEC 27001 e ISO/IEC 27002. Alineado con ISO/IEC 27005, la guía cumple una serie de pasos en cada una de las actividades propuestas, las cuales en conjunto conforman el proceso de gestión del riesgo según lo muestra la figura 1.

El proceso es cíclico con el fin de redefinir sus fases ante un incidente o evento de seguridad que no fue controlado satisfactoriamente y para una actualización o revisión periódica preventiva de carácter obligatorio ajustándose a los cambios de la organización y del entorno. Esta característica determina un análisis en profundidad de los riesgos presentes y permite racionalizar los controles a implementar hasta llevar el riesgo a niveles aceptables por la organización. Se destaca en la figura 1 que las actividades están sujetas en todo momento a la divulgación a la alta Dirección y al personal involucrado. Las fases del proceso son:

- Establecimiento del contexto: Es la primera actividad donde inicia el proceso. Para su desarrollo es indispensable conocer muy bien la organización y contar con toda la información estratégica sobre el negocio. Así se definen los criterios básicos, se establece el alcance y límite y se define la estructura y responsabilidades para la gestión del riesgo en la compañía.

- Valoración del riesgo: Hacen parte de esta fase el análisis y la evaluación del riesgo. La primera incluye la identificación y la estimación del riesgo en las cuales se identifican activos de información, amenazas, vulnerabilidades y consecuencias. Por la otra parte se identifican escenarios incidentes y se asignan valores a la probabilidad de ocurrencia y a las consecuencias de tales riesgos bajo criterios definidos en el contexto. La segunda etapa,

también bajo criterios definidos en el contexto, determina el nivel del riesgo bajo una escala y permite priorizar su atención. Si toda la información anterior es suficiente para caracterizar los riesgos y determinar claramente las acciones a implementar en busca de niveles aceptables, la primera decisión del flujo llevará a la siguiente fase, de lo contrario se llevará a cabo otra iteración para redefinir actividades previas.

- Tratamiento del riesgo: En esta instancia se concretan las acciones a tomar sobre los riesgos valorados, es decir, se seleccionan los controles de acuerdo a lo planteado en el contexto según corresponda al objetivo y necesidades de la organización: reducir, retener, evitar o transferir el riesgo, lo anterior de acuerdo al costo de implementación de las opciones y los beneficios esperados. Si el tratamiento no es satisfactorio según lo esperado por la Compañía el segundo punto de decisión del flujo permite redefinir las etapas anteriores con las iteraciones que sean necesarias hasta lograr el riesgo residual o el nivel de riesgo que es aceptado para la Organización.

- Aceptación del riesgo: Esta actividad formaliza la declaración de la alta Dirección de la organización para asumir el riesgo residual o el riesgo tolerable con el fin de soportar y documentar las opciones de tratamiento, especialmente aquellas que por situaciones determinantes (por ejemplo altos costos) se omiten o posterga la implementación de controles, o sea, aquellos que no satisfacen los criterios normales definidos en el contexto. Es la parte final del ciclo normal y el siguiente paso es comunicarlo y monitorearlo.

- Comunicación del riesgo: Formaliza y divulga ante la alta Dirección, al personal involucrado en el proceso y ante la Organización en general, las actividades realizadas sobre la valoración y tratamiento del riesgo facilitando la toma de decisiones al ritmo de los cambios del negocio y al estado del SGSI. Esta etapa envía y/o recibe actualizaciones de cada fase del proceso según corresponda.

- Monitoreo y revisión del riesgo: Hace parte de la fase verificar del ciclo P-H-V-A del SGSI. Considerando que los riesgos son cambiantes, esta actividad permite una alineación continua entre el proceso de gestión del riesgo y los cambios que afectan la Organización y su entorno. Conforma la calidad y mejora continua del proceso.

A continuación se hace una descripción de cómo se alinea la guía con cada fase del ciclo P-H-V-A.

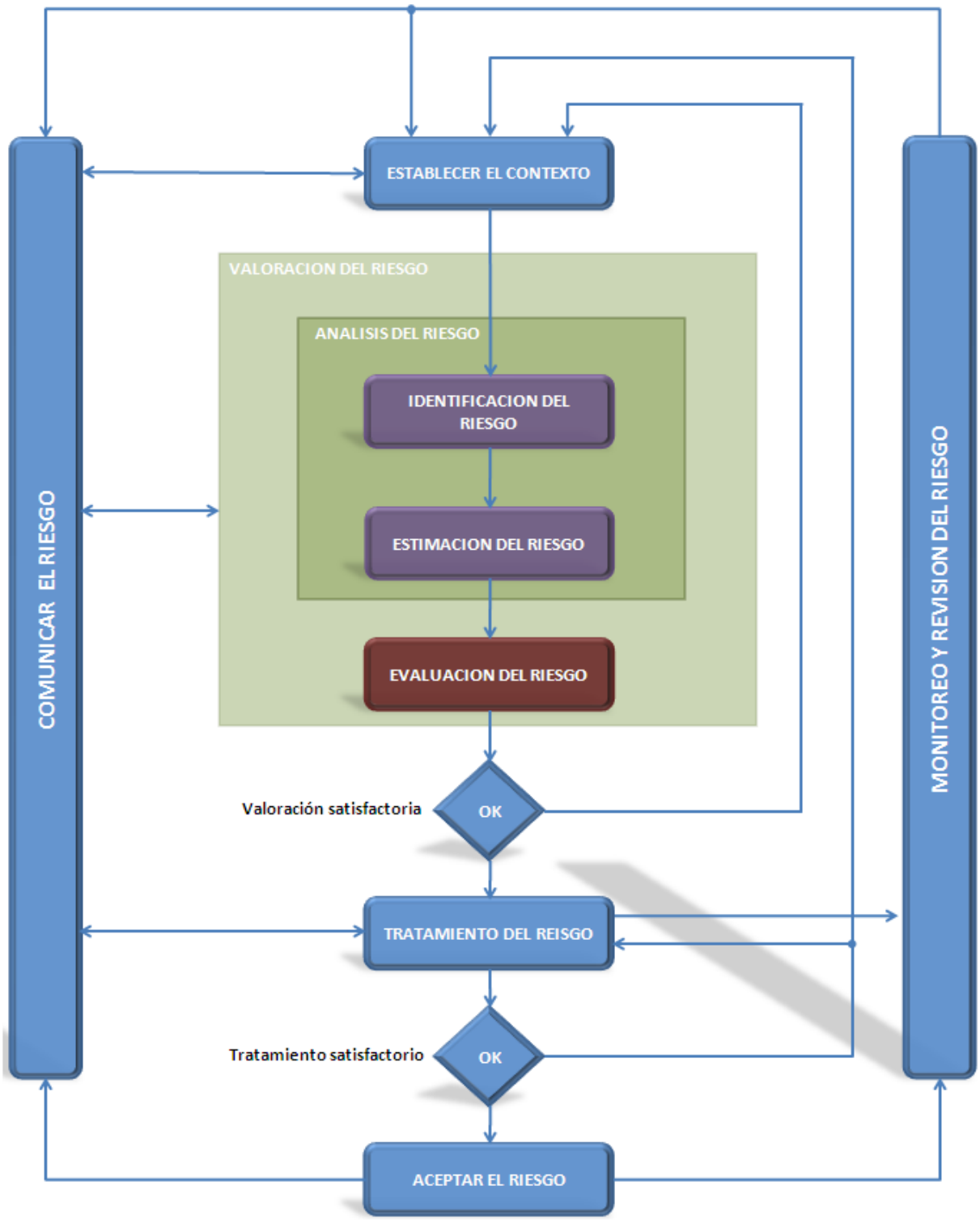
La guía plantea procesos de mejora continua involucrando interacciones hasta lograr reducción de los riesgos en niveles aceptables por la organización. Inicia con la planeación, donde se plantea un conocimiento detallado de la organización y sus requisitos de seguridad de la información como punto importante de partida para realizar los siguientes procesos:

- El diagnóstico. En el cual se examina el cumplimiento entre lo implementado en su SGSI y el estándar ISO/IEC 27001 de tal forma que permita conocer las actividades a gestionar para cumplir con lo exigido por el sistema. Este proceso determinará el estado de cumplimiento de la norma para las actividades incluidas en el mapa de procesos de la compañía y promueve el diseño de un modelo de gestión para llevarlas a un nivel de cumplimiento aceptable. Este será el punto de partida de la presente guía.

- Análisis, valoración, tratamiento, aceptación, comunicación y monitoreo de los riesgos. Se incluye como valor agregado y opcional la elaboración de un plan de continuidad del negocio.

Enseguida la fase Hacer abarca el tratamiento de riesgos, mediante las etapas monitoreo-revisión y comunicación del mismo se alcanza las fases verificar y actuar gracias a la medición de la eficacia de las medidas implementadas y a las interacciones cíclicas del proceso sobre acciones de mejora que permitirán inclusive redefinir la fase planear periódicamente o ante un incidente o evento de seguridad.

Figura 17: Proceso Gestión del Riesgo ISO/IEC 27005.



Fuente: Proyecto de Norma Técnica Colombiana NTC-ISO/IEC 27001.

3. ETAPA I: IDENTIFICACIÓN Y EVALUACIÓN PARA EL TRATAMIENTO DE LOS RIESGOS.

3.1 Reunir requisitos para esta actividad.

Validar que las fases análisis y diagnóstico SGSI y Organización de la Seguridad están cumplidas y documentadas.

3.2 Ejecutar acción.

5.2.1. Definir procesos que harán parte de la Gestión del Riesgo.

5.2.2. Definir requisitos de seguridad.

5.2.3. Asignar presupuesto, estimación de alto nivel de los recursos económicos y reservarlos con el fin de implantar y mantener el proceso de Gestión del Riesgo.

5.2.4. Valorar los Riesgos.

- Analizar los riesgos. En esta fase se encuentran, enumeran y se caracterizan los riesgos a los que se considera que está expuesta la organización.

  - Identificar activos de información.
  - Realizar análisis de estadísticas históricas sobre incidentes o eventos de seguridad.
  - Identificar los riesgos: Identificar amenazas, vulnerabilidades, consecuencias y controles existentes.
  - Estimar los riesgos: Asignar valores a la probabilidad de ocurrencia y a las consecuencias de un riesgo para estimar su valor en los posibles escenarios de incidentes aplicando el método ***Determinación del valor para la probabilidad y las consecuencias posibles de los riesgos.***

- Evaluar los riesgos.

  - Definir los criterios de clasificación del riesgo basados en las condiciones propias del negocio.
  - Filtrar la valoración de riesgos entregada por los dueños de los procesos para evitar subjetividad y reclasificarla si es necesario de acuerdo a los criterios definidos.
  - Priorizar los riesgos sobre los sistemas de la organización aplicando el concepto ***Organización = Sistema 1 + Sistema 2 + … + Sistema n.***
  - Comparar el riesgo estimado contra criterios de clasificación dados para determinar su importancia.

5.2.5. Alimentar la fase de comunicación del riesgo midiendo el alcance y restricciones al público destino.

5.2.6. Alimentar el plan de comunicación y sensibilización organizacional midiendo el alcance y restricciones al público destino.

3.3 Documentar resultados.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

4. ETAPA II: SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES.

4.1 Reunir requisitos para esta actividad.

Validar que la fase Valoración del Riesgo está cumplida satisfactoriamente y ha sido documentada.

4.2 Ejecutar Acción.

4.2.1. Plan de Continuidad del negocio (PCN). Si fue considerado por la alta dirección, definir, implementar y aprobar los procedimientos y estrategias que aseguren la continuidad oportuna y ordenada de los procesos críticos de la organización con niveles aceptables por los clientes.

- Definir el proyecto.
- Valorar los riesgos.
- Asignar el tiempo objetivo de recuperación RTO.
- Asignar el punto objetivo de recuperación RPO.
- Diseñar el plan de estrategias.
- Realizar la fase de pruebas, mantenimiento y mejora del proyecto.
- Capacitar al grupo de trabajo, divulgar y sensibilizar toda la organización.
- Realizar documentación final: gestión de incidentes, plan de emergencias, plan de comunicación de crisis, plan de recuperación de desastres.

4.2.2. Analizar si la valoración del riesgo fue satisfactoria.

- Definir si luego de la primera iteración del flujo gestión del riesgo se cuenta con información suficiente para concretar en la siguiente fase las opciones de tratamiento que permitirán dejarlos en un nivel aceptable para la organización.
- Definir si luego de la primera iteración del flujo gestión del riesgo es necesario otra iteración del flujo para redefinir el contexto.

- Definir si se debe realizar otra iteración del flujo gestión del riesgo debido a revisión periódica del proceso cada seis meses o por un evento o incidente de seguridad no tratado satisfactoriamente.

4.2.3. Tratar los riesgos sobre los activos de información.

- Según resultado de la fase Evaluación del riesgo, se debe realizar un análisis de cumplimiento de los objetivos de control y controles listados en la norma ISO/IEC 27002 en el orden indicado: 5. POLÍTICA DE SEGURIDAD, 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, 13. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN, 14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO, 8. SEGURIDAD DE LOS RECURSOS HUMANOS, 11. CONTROL DE ACCESO, 15. CUMPLIMIENTO, 10. GESTIÓN DE COMUNICACIONES Y OPERACIONES, 12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN, 7. GESTIÓN DE ACTIVOS, 9. SEGURIDAD FÍSICA Y DEL ENTORNO, finalmente Objetivos relacionados a directrices propias para cubrir necesidades particulares que no estén incluidos en la norma, estos deberán clasificarse en un dominio afín de la norma para facilitar la trazabilidad.

- Determinar la totalidad de los controles nuevos, existentes y/o propios que son necesarios y contribuyen al cumplimiento de los objetivos de control.

- Determinar factor común de la totalidad de controles necesarios frente a los objetivos de control para evitar redundancia.

- Determinar compendio de la mejor alternativa de los controles en función de cumplimiento y costo-beneficio.

- Realizar un filtro a los controles seleccionados basado en las restricciones relacionadas.

- Justificar y documentar las razones por las cuales algún objetivo de control y/o controles listados en ISO/IEC 27002 son excluidos.

- Realizar análisis del presupuesto requerido para la implantación de los controles (existentes o planificados) sin ningún tipo de reserva o limite, fijando un periodo anual.

- Aprobación de la alta dirección por el presupuesto y listado definitivo de controles a implementar y mantener.

- Analizar si luego de esta decisión se presentan nuevos riesgos y por lo tanto se debe realizar una redefinición de todo el ciclo gestión del riesgo.

- Asignar responsable idóneo a cada control seleccionado.

- Generar documento Declaración de Aplicabilidad aprobado por la alta dirección.

- Aprobado por la alta dirección, proyectar la opción de tratamiento de riesgos a cada activo de información en orden de criticidad en función de los escenarios incidentes y el impacto al negocio según la fase evaluación del riesgo y según metodología establecida : 1. Retener, 2. Evitar, 3. Reducir, 4. Transferir, 5. Combinación de opciones.

- Definir indicadores para medida de eficiencia de los controles y metas a cumplir.

- Diseñar y realizar pruebas controladas a las salvaguardas para comprobar su rendimiento de forma preventiva.

- Diseñar registro de control al desempeño de los controles implantados.

- Recopilar y analizar los resultados parciales y/o finales de los indicadores de rendimiento de todos los controles.

- Documentar aprobación de la alta dirección sobre el riesgo residual obtenido luego del periodo de gestión del riesgo o si no cumple las expectativas de la organización, la autorización para revisar o redefinir las fases de gestión del riesgo que sean necesarias.

4.2.4. Alimentar la fase de comunicación del riesgo midiendo el alcance y restricciones al público destino.

4.2.5. Alimentar el plan de comunicación y sensibilización organizacional midiendo el alcance y restricciones al público destino.

4.3 Documentar resultados.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

5. ETAPA III: MEDICIÓN DE EFICACIA DE LOS CONTROLES.

5.1 Reunir requisitos para esta actividad.
Validar que la fase Tratamiento del Riesgo está cumplida satisfactoriamente y ha sido documentada.

5.2 Ejecutar acción.

5.2.1. Analizar si el plan de tratamiento del riesgo fue satisfactorio y es aceptado. Basado en los resultados de las fases identificación, estimación y evaluación del riesgo para el periodo bajo prueba o movido por un evento o incidente se seguridad, la alta dirección y el grupo SGSI debe analizar, documentar y aprobar:

- Cuáles riesgos tratados se han reducido a niveles aceptables y cumplen las expectativas de seguridad de las partes interesadas continuando así con las siguientes fases del proceso.

- Sobre los riesgos tratados pero que se mantienen en niveles intolerables, decidiendo si se debe redefinir solamente la fase de tratamiento o realizar varias iteraciones del ciclo hasta obtener resultados satisfactorio.

- Si se aceptan ciertos riesgos sin tratamiento o tratados pero por encima de niveles aceptables para la organización (por beneficios indirectos o costos de tratamiento demasiado altos) continuando así con las siguientes fases del proceso.

5.2.2. Alimentar la fase de comunicación del riesgo midiendo el alcance y restricciones al público destino.

5.2.3. Alimentar el plan de comunicación y sensibilización organizacional midiendo el alcance y restricciones al público destino.

5.3 Documentar resultados.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

6. ETAPA IV: SEGUIMIENTO, REVISIÓN Y VALORACIÓN PERIÓDICA DE RIESGOS.

6.1 Reunir requisitos para esta actividad.

Validar que la fase Tratamiento del Riesgo está cumplida satisfactoriamente y ha sido documentada.

6.2 Ejecutar acción.

6.2.1. Comunicar el riesgo.

- A través de un comité principal realizado por integrantes del grupo SGSI y con frecuencia mensual, generar un plan de comunicaciones que se aplique en cada instancia del flujo de gestión del riesgo de tal forma que permita al

equipo de trabajo comprensión continua de las actividades, además de revisar avances, resultados, alinear y aclarar planes y decisiones entre el grupo SGSI, la alta dirección y los dueños de los procesos. Documentar y registrar actas de reunión.

- A través de un comité secundario realizado entre los dueños de los procesos y sus equipos de trabajo, donde se mide el alcance y las restricciones para divulgar la información sobre el proceso de gestión del riesgo, dar continuidad a los objetivos del comité principal. Documentar y registrar actas de reunión.

- Las actas resultados de los comités deben contener acuerdos, planes de acción y de mejora, identificar responsables y niveles de escalamiento por las acciones definidas en los nuevos planes, ajustar y documentar conforme a las mejoras identificadas el proceso completo de gestión del riesgo, implementar las acciones acordadas, revisar el avance de implementación de los nuevos planes y del proceso en general.

6.2.2. Monitoreo y revisión del riesgo. Documentar acciones que evidencien la supervisión y redefiniciones del proceso de gestión del riesgo. Analizar los resultados y documentar las acciones tomadas de forma preventiva y correctiva frente a:

- Durante el periodo de ejecución definido para el proceso y en cada instancia del mismo.
- Ante un incidente o evento de seguridad.
- Ante cambios en el mapa de procesos de la organización.
- Ante modificación de los requisitos de seguridad.
- Reforma importante en el organigrama de la organización.
- Cambios en la asignación presupuestal para la gestión del riesgo.
- Valoración del riesgo no satisfactoria.
- Tratamiento del riesgo no satisfactorio.
- Indicadores de eficiencia de controles implantados.

6.2.3. Alimentar la fase de comunicación del riesgo midiendo el alcance y restricciones al público destino.

6.2.4. Alimentar el plan de comunicación y sensibilización organizacional midiendo el alcance y restricciones al público destino.

6.2.5. Consolidar Plan de Comunicación y Sensibilización Organizacional. Con los insumos recibidos por cada fase del proceso de gestión del riesgo, el grupo SGSI con el apoyo de las áreas de comunicación de la compañía realizan esta labor mediante campañas promotoras internas vía carteleras, intranet, correo electrónico, agenda en comités de área, etc. Se documentan todas las acciones tomadas al respecto en la carpeta del plan.

6.3 Documentar resultados.

Los resultados finales y las debidas actualizaciones son consolidados en un único documento tipo carpeta, separados e identificados bajo un índice por la fase o numeral de la guía permitiendo trazabilidad a la gestión y facilitando consultar la información requerida.

ANEXO A

DESCRIPCIÓN DETALLADA DE LAS ACTIVIDADES DE CADA ETAPA DE LA GESTIÓN DEL RIESGO

A.1 DIAGNÓSTICO INICIAL DEL SGSI EN LA ORGANIZACIÓN

El diagnóstico inicial a realizar en la organización está contenido en la actividad Establecer el Contexto del proceso Gestión del Riesgo mostrado anteriormente en la figura 1 y abarca todos los temas de las cuatro fases de la guía.

A.1.1 Requisito

Compromiso de la alta Dirección para realizar el diagnóstico. Considerando que la Organización puede no tener en marcha ningún sistema de gestión, que está en proceso de implementación o por el contrario ya esté en funcionamiento alguno, corresponde a la alta Dirección liderar esta fase en conjunto con el administrador del sistema implementado o a quien delegue según sea el caso. Mediante acta de reunión, la Dirección aprueba el inicio de las actividades correspondientes a esta fase y asigna los responsables de ejecución, seguimiento y análisis.

A.1.2 Acción

A.1.2.1 Toma de datos.

En esta etapa de la implementación del SGSI en la compañía, se recomienda iniciar conociendo el estado de las actividades, procesos o procedimientos que estén relacionados con lo requerido por la norma. Para ello se debe realizar un análisis de cumplimiento entre lo implementado en su Sistema Integral de Gestión y el estándar ISO/IEC 27001 basados inicialmente en los procesos y procedimientos del mapa de procesos de la compañía y luego en el grupo de

actividades que aún no están documentadas formalmente como parte del Sistema Integral de Gestión.

Como herramienta de apoyo para el levantamiento de información se ha diseñado un cuadro que abarca todos los puntos requeridos por el estándar ISO/IEC 27001 en la fase Planear, la cual es la fase que corresponde a este proyecto, trabajando los capítulos 4.2.1 Establecimiento y Gestión SGSI, 4.2.2 Implementación y Operación SGSI, 4.2.3 Seguimiento y Revisión SGSI y 4.2.4 Mantenimiento y Mejora SGSI.

En el cuadro se señala el numeral de la norma al cual corresponde la variable que se va a medir y también la fase del ciclo PHVA a la que pertenece. De cada variable se debe definir cualitativamente un Estado Actual que describa cómo se aplica dicha variable en la compañía y las tareas que se llevan a cabo para que sirvan como referencia durante la implementación de la norma. Se le debe dar también una ponderación cuantitativa con valores de 0 a 4, donde 0 representa ningún avance o cumplimiento de la variable medida, y 4 significa total cumplimiento. Finalmente se encuentra una casilla para calificar cualitativamente el Estado Final de la variable una vez se haya implementado el SGSI y con base en esto poder verificar el cumplimiento de cada uno de los requerimientos de la norma y también para mostrar el trabajo realizado con base en el Estado Actual. Se incluye una casilla de observaciones que será útil para cualquier comentario relacionado con la medición o implementación de la variable respectiva.

Cuadro 7: Formato para diagnóstico basado en la norma ISO/IEC 27001.

FASE SGSI	NUMERAL	CICLO PROCESO	VARIABLE	ESTADO ACTUAL	PONDERACIÓN	ESTADO FINAL	OBSERVACIONES
1	4.2.1	P	**ESTABLECIMIENTO Y GESTIÓN SGSI**				
1	4.2.1.a	P	**ALCANCE Y LIMITES DEL SGSI**				
1	4.2.1.a	P	¿Están definidas las características del negocio?				
1	4.2.1.a	P	¿Están definidos los Objetivos y necesidades de la Organización?				
1	4.2.1.a	P	¿Está definida la Estructura y recursos en la Organización para implantar el SGSI?				

1	4.2.1.a	P	¿Se han seleccionado las áreas/procesos a involucrar en el SGSI?				
1	4.2.1.a	P	¿Están definidos los requisitos y expectativas de seguridad?				
1	4.2.1.a	P	¿Están definidas las actividades, sedes físicas, tecnología a incluir/excluir en el SGSI?				
FASE SGSI	**NUMERAL**	**CICLO PROCESO**	**VARIABLE**	**ESTADO ACTUAL**	**PONDERACIÓN**	**ESTADO FINAL**	**OBSERVACIONES**
1	4.2.1.a	P	¿Se han estimado los recursos humanos, técnicos y económicos para implantar el SGSI?				
1	4.2.1.a	P	¿Existe un Documento Alcance y Límites SGSI?				
2	4.2.1.b	P	**POLÍTICA DE SEGURIDAD**				
2	4.2.1.b	P	¿Se ha definido una política de seguridad y objetivos globales?				
2	4.2.1.b	P	¿Existe declaración de la Dirección para el apoyo de objetivos y principios de seguridad?				
2	4.2.1.b	P	¿Están explicadas las políticas?				
2	4.2.1.b	P	¿Existe una definición de responsabilidades generales y especificas en cada rol?				
2	4.2.1.b	P	¿Están definidos los activos que se protegen, de quién/qué y por qué?				
2	4.2.1.b	P	¿Se han establecido los criterios para gestión de riesgos y selección de objetivos de control y controles?				
2	4.2.1.b	P	¿Se han seleccionado las medidas de seguridad a implementar?				
2	4.2.1.b	P	¿Se han establecido los criterios de actuación ante incidentes de seguridad?				
2	4.2.1.b	P	¿Se han establecido los procesos de revisión periódica, ante incidentes de seguridad o ante cambios estructurales en la organización?				
2	4.2.1.b	P	¿Se ha publicado y aprobado la política de seguridad por parte de la Dirección?				

2	4.2.1.b	P	¿Está disponible la política de seguridad para consulta?				
2	4.2.1.b	P	¿Existe Documento Política de Seguridad?				
3	4.2.1.a	P	**ORGANIZACIÓN DE LA SEGURIDAD**				
3	4.2.1.a	P	¿Se ha seleccionado al responsable de la seguridad?				
FASE SGSI	**NUMERAL**	**CICLO PROCESO**	**VARIABLE**	**ESTADO ACTUAL**	**PONDERACIÓN**	**ESTADO FINAL**	**OBSERVACIONES**
3	4.2.1.a	P	¿Se ha nombrado al Comité de Dirección?				
3	4.2.1.a	P	¿Se ha nombrado al Comité de Gestión?				
3	4.2.1.a	P	¿Se han tomado medidas frente a terceros para proteger la información?				
3	4.2.1.a	P	¿Existe Documento Organización de la Seguridad?				
4	4.2.1.a	P	**SENSIBILIZACIÓN Y FORMACIÓN DEL PERSONAL**				
4	4.2.1.a	P	¿Existe una campaña para divulgar los avances del SGSI en toda la organización?				
4	4.2.1.a	P	¿Se ha capacitado al personal encargado de la SGSI para enfrentar sus nuevas actividades?				
4	4.2.1.a	P	¿Existe Documento sensibilización y formación del personal?				
5	4.2.1.d	P	**IDENTIFICACIÓN DE ACTIVOS**				
5	4.2.1.d	P	¿Se ha definido alguna metodología para identificar activos?				
5	4.2.1.d	P	¿Existe inventario de activos (descripción-localización-propietario-grado de seguridad)?				
5	4.2.1.d	P	¿Están incluidos los activos intangibles (Imagen Organizacional)?				
5	4.2.1.d	P	¿Se ha determinado el ciclo de vida útil de los activos?				
5	4.2.1.d	P	¿Existe análisis o árbol de dependencia entre activos?				

5	4.2.1.d	P	¿Existe Documento Inventario de activos?				
6	4.2.1.d	P	**VALORACIÓN DE ACTIVOS**				
6	4.2.1.d	P	¿Existe valoración de activos según la importancia e impacto ante una incidencia basado en Confidencialidad, Integridad y Disponibilidad de la información (cuantitativa y/o cualitativa)?				
FASE SGSI	**NUMERAL**	**CICLO PROCESO**	**VARIABLE**	**ESTADO ACTUAL**	**PONDERACIÓN**	**ESTADO FINAL**	**OBSERVACIONES**
6	4.2.1.d	P	¿Se ha definido algún método para valorar activos (entrevista, encuesta)?				
6	4.2.1.d	P	¿Existe Documento valoración de activos?				
7	4.2.1.d	P	**IDENTIFICACIÓN DE RIESGOS**				
7	4.2.1.d	P	¿Se han identificado áreas que requieren medidas de seguridad?				
7	4.2.1.d	P	¿Existe identificación de riesgos y están asociados a los activos inventariados?				
7	4.2.1.d	P	¿Existe identificación de riesgos asociados a los activos más críticos?				
7	4.2.1.d	P	¿Hay Amenazas identificadas que afectan los activos inventariados?				
7	4.2.1.d	P	¿Existe Análisis de vulnerabilidades de los activos inventariados?				
7	4.2.1.d	P	¿Se conoce el impacto por la materialización de un riesgo?				
7	4.2.1.e	P	¿Se ha determinado la probabilidad de ocurrencia de un riesgo?				
7	4.2.1.d	P	¿Este proceso considera los recursos de la organización?				
7	4.2.1.d	P	¿Existe Análisis de medidas de seguridad ya implantadas?				
7	4.2.1.d	P	¿Hay Participación de las diversas áreas de la compañía?				
7	4.2.1.d	P	¿Existe Documento identificación de riesgos?				
8	4.2.1.c	P	**ENFOQUE PARA VALORACIÓN DE RIESGOS**				
8	4.2.1.c	P	¿Se ha definido alguna metodología para valorar riesgos?				
8	4.2.1.c	P	¿Se han estimado los niveles para los riesgos?				

8	4.2.1.c	P	¿Existe un Documento enfoque para valorar riesgos?				
9	4.2.1.f	P	**GESTIÓN DEL RIESGO**				
9	4.2.1.f	P	¿Se han definido acciones frente a los riesgos identificados y valorados?				
9	4.2.1.f	P	¿Se ha determinado el riesgo residual para cada riesgo identificado y valorado?				

FASE SGSI	NUMERAL	CICLO PROCESO	VARIABLE	ESTADO ACTUAL	PONDERACIÓN	ESTADO FINAL	OBSERVACIONES
9	4.2.1.c,e	P	¿Existen criterios definidos para tomar riesgo aceptable?				
9	4.2.1.f	P	¿Hay Aprobación por dirección para los riesgos aceptable?				
9	4.2.1.f	P	¿Existe Documento de Aprobación Dirección Gestión de Riesgos?				
9	4.2.1.h	P	¿Existe Documento de Aprobación Dirección Riesgos residuales?				
9	4.2.1.f	P	¿Existe Documento matriz de riesgos?				
10	4.2.1.g	P	**SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES**				
10	4.2.1.g	P	¿Existe Análisis de controles existentes?				
10	4.2.1.g	P	¿Existe Análisis y selección de los dominios, objetivos y controles a implantar?				
10	4.2.1.g	P	¿Se Cumplen los requisitos definidos en procesos de tratamiento de riesgos?				
10	4.2.1.g	P	¿Se hacen Inversiones en controles proporcionales al impacto del riesgo?				
10	4.2.1.g	P	¿Existen Controles documentados en procedimientos?				
10	4.2.1.g	P	¿Hay disponibilidad de recursos para implementar los controles?				
10	4.2.1.g	P	¿Existe justificación para los objetivos y controles seleccionados y no seleccionados?				
10	4.2.1.j	P	¿Existe Documento declaración de aplicabilidad?				
11	4.2.1.i	P	**AUTORIZACIÓN PARA IMPLEMENTAR Y OPERAR SGSI**				

11	4.2.1.i	P	¿Existe Documento de aprobación por dirección para implementar y operar el SGSI?				
12	4.2.1	P	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (PCN)**				
12	4.2.1	P	¿Están identificados los procesos críticos a recuperar progresivamente?				
12	4.2.1	P	¿Existe PCN extraído de gestión de riesgos críticos?				
12	4.2.1	P	¿Se ha puesto a prueba el PCN (cuánto es el tiempo de recuperación mínimo, los Acuerdos de Niveles de Servicio (ANS) se conservan)?				
FASE SGSI	**NUMERAL**	**CICLO PROCESO**	**VARIABLE**	**ESTADO ACTUAL**	**PONDERACIÓN**	**ESTADO FINAL**	**OBSERVACIONES**
12	4.2.1	P	¿Existe comité de emergencia para solucionar las crisis?				
12	4.2.1	P	¿Existen procedimientos (relacionados a cada situación) establecidos para aplicar en las crisis (indica acciones y sugerencias)?				
12	4.2.1	P	¿Los procedimientos han sido divulgados y puestos a prueba?				
12	4.2.1	P	¿Existen registros que documentan la reacción ante la crisis y su respectivo análisis?				
12	4.2.1	P	Fases PCN: Definición del proyecto (alcance y objetivos de peor escenario) - Análisis de impacto (riesgos, impacto económico) - Selección de estrategias (recursos-salvaguardas a usar)-Desarrollo - Pruebas periódicas y mantenimiento				
13	4.2.2	H	**IMPLEMENTACIÓN Y OPERACIÓN SGSI**				
13	4.2.2.a,b	H	**PLAN DE TRATAMIENTO DE RIESGOS**				
13	4.2.2.a,b	H	¿Existe guía de ejecución del plan para tratamiento de riesgos?				
13	4.2.2.h	H	¿Se han definido Procedimientos y controles adicionales para detectar y reaccionar ante incidentes de seguridad en esta fase?				
13	4.2.2.a,b	H	¿Existe documento informe de plan para tratamiento de riesgos?				
13	4.2.2.c	H	**IMPLANTACIÓN DE CONTROLES**				

13	4.2.2.c	H	¿Se han definido los responsables de los controles técnicos?				
13	4.2.2.c	H	¿Se han definido los responsables de los controles administrativos?				
13	4.2.2.d	H	¿Se han definido los indicadores para cada control implantado?				
13	4.2.2.d	H	¿Existe un método para medir la eficacia de los controles implantados?				
13	4.2.2.h	H	¿Se han implantado controles adicionales ante incidentes de seguridad detectados en esta fase?				
13	4.2.2.e	H	¿Se ha hecho sensibilización y divulgación?				
FASE SGSI	**NUMERAL**	**CICLO PROCESO**	**VARIABLE**	**ESTADO ACTUAL**	**PONDERACIÓN**	**ESTADO FINAL**	**OBSERVACIONES**
13	4.2.2.c	H	¿Existe un documento informe de implantación de controles (cuadro de mando)?				
14	4.2.3	V	**SEGUIMIENTO Y REVISIÓN SGSI**				
14	4.2.3	V	**PROCEDIMIENTOS SEGUIMIENTO Y REVISIÓN**				
14	4.2.3.a,c	V	¿Se hace un análisis periódico de indicadores y su eficacia?				
14	4.2.3.b,e	V	¿Se realizan auditorías internas/externas al sistema?				
14	4.2.3.b,e	V	¿Se hace revisión por Dirección de las auditorias?				
14	4.2.3.a	V	¿Se hace revisión por Dirección del informe Comité de Gestión?				
14	4.2.3.a	V	¿Se hace revisión por Dirección del informe Responsable Seguridad?				
14	4.2.3.d	V	¿Se hace revisión periódica por Dirección de valoración de riesgos, riesgo residual, riesgo aceptable?				
14	4.2.3.b,e	V	¿Existe un documento auditorías internas?				
14	4.2.3.a,b,c,d,e	V	¿Existe un documento donde se evidencie la revisión de auditorías por parte de la dirección?				

15	4.2.4	A	**MANTENIMIENTO Y MEJORA SGSI**				
15	4.2.4.a,b	A	¿Se ejecutan acciones correctivas, preventivas, mejora?				
15	4.2.4.a,b	A	¿Se hace la actualización de riesgos y controles?				
15	4.2.4.d	A	¿Se hace la medición de eficacia de acciones implementadas?				
15	4.2.4.c	A	¿Existe un documento informe de ejecución de acciones correctivas-preventivas?				

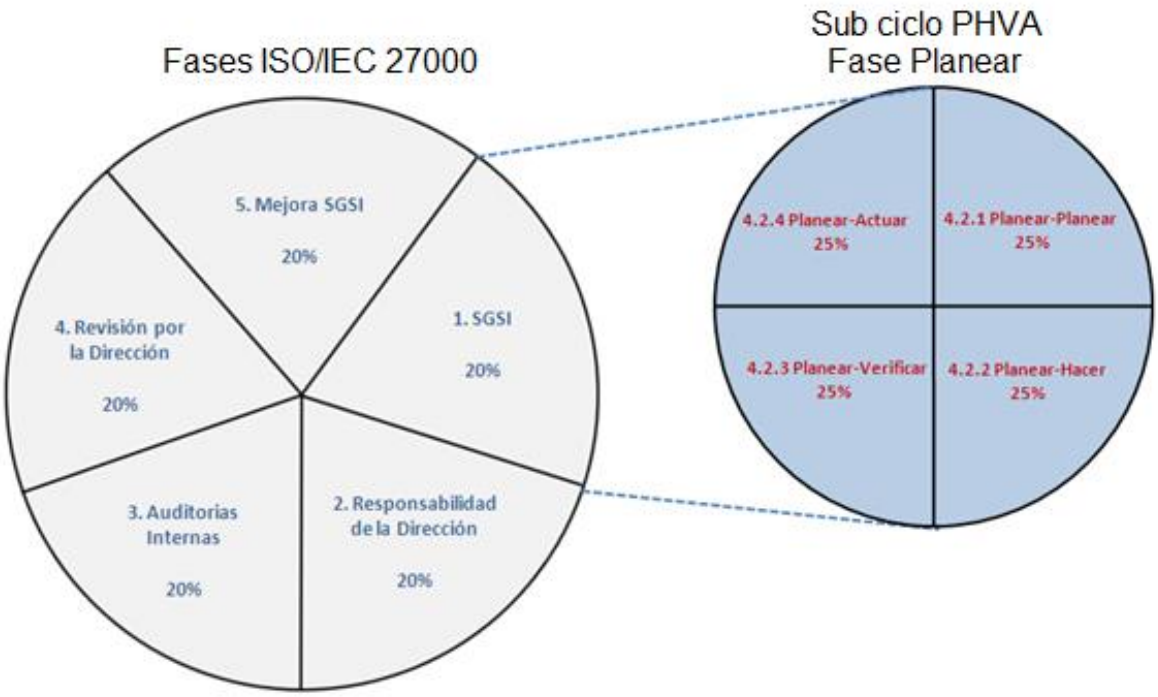
Fuente: Los autores.

A.1.2.2 Cálculo del avance de implementación del SGSI.

Según lo muestra la figura 2, la norma ISO/IEC 27001 incluye cinco aspectos: SGSI, Responsabilidad de la Dirección, Auditorías Internas, Revisión por la Dirección y Mejora SGSI. Para el análisis de la información levantada para el diagnóstico se da igual peso porcentual a cada aspecto, es decir, 20%.

Dado que la fase que se analiza en este proyecto es la fase Planear y que para obtener una mejor representación de esta es necesario abordarla como un subsistema que contiene a su vez un ciclo PHVA, se introduce entonces los conceptos de sub ciclos Planear-Planear, Planear-Hacer, Planear-Verificar y Planear-Actuar con un peso individual de 25%, de tal forma que se pueda evaluar cada uno por separado y también la fase Planear completa respecto a todo el sistema SGSI.

Figura 18: Fases de la norma ISO/IEC 27001 y subcapítulos de la fase Planear



Fuente: Proyecto de Norma Técnica Colombiana NTC-ISO/IEC 27001 – Los autores.

Teniendo en cuenta la definición del sub ciclo PHVA para la fase Planear del SGSI y las calificaciones obtenidas en el levantamiento de información del diagnóstico, se muestra a continuación la metodología propuesta para calcular el avance en la implementación de la fase tratada como parte del SGSI.

Cada una de las variables del diagnóstico fueron calificadas de 0 a 4, donde 0 representa ningún avance o ejecución de la tarea, 4 una ejecución total, 2 un punto medio y 1 y 3 puntos de avance intermedio que describen mejor y con más exactitud el estado real de cada una de las variables medidas.

El estado de cada una de las fases del sub ciclo PHVA se calcula sumando todas las calificaciones obtenidas dentro de esa fase y dividiéndola sobre el total de puntos máximos posibles de ella. Ejemplo: Según el cuadro 1, el sub ciclo Planear-Planear (numeral 4.2.1) posee 75 variables que podrían sumar, en el mejor de los casos, un puntaje máximo de 300 (75x4). Al sumar los puntajes asignados a cada una de las variables dentro de la sub fase Planear-Planear,

dividirlo entre 300 y multiplicarlo por 100%, se obtiene el porcentaje de avance de esa sub fase específica respecto a la fase Planear del SGSI.

Una vez se haya calculado el avance de cada una de las sub fases, se multiplica cada resultado por el 20% el cual corresponde al peso de la fase Planear como parte de todo el SGSI y se suman los cuatro resultados, obteniendo así el porcentaje de avance de la fase Planear general.

A.1.2.3 Análisis del diagnóstico.

Este primer acercamiento al estado inicial de la compañía que se enfrenta a la implantación del SGSI, brinda herramientas importantes para la gestión de los recursos requeridos ante la dirección y para identificar así mismo las tareas de mayor exigencia, logrando obtener una visión global de todo el proceso de implementación y certificación en la norma.

Como parte de la metodología de las guías que se definen en este proyecto, se debe hacer un resumen de los principales hallazgos del diagnóstico, buscando definir claramente las tareas a ejecutar para el cumplimiento de cada uno de los requisitos de la norma, organizándolos según las fases y variables del cuadro 1 y teniéndolos como base para la creación del cronograma de implementación del SGSI.

Una manera organizada entonces de identificar estos hallazgos es bajo la siguiente nomenclatura:

SGSI-P-X-YY, donde
SGSI: Sistema de Gestión de Seguridad de la Información.
P: Fase Planear del SGSI en general. Es el alcance de este proyecto.
X: Sub ciclo de la fase Planear (PHVA).
YY: Número consecutivo para identificación del hallazgo específico.

Ejemplo:

SGSI-P-P-01: *No están definidos los requisitos ni expectativas de seguridad incluyendo las sedes de la compañía, tecnología, o procesos que se excluyen del SGSI.*

Sería normal que en la región las compañías que están trabajando para la implementación y certificación de la norma ISO27001, tengan ya implementada o en marcha su certificación del Sistema de Gestión de Calidad ISO9001 (SGC).

Es necesario administrar el SGSI bajo un modelo de gestión como el propuesto en la figura 10 el cual se basa en las recomendaciones de la norma ISO27000, se busca complementar el alcance del SGC para que aplique al SGSI mediante ajustes a los procedimientos que permiten cumplir los requisitos establecidos en la norma ISO9001 y conformar así un sistema de gestión integral para no repetir esfuerzos ni sobrecargar de actividades los procesos. El modelo está basado en el ciclo P-H-V-A como pilar de la gestión de actividades aplicable a cada componente y de igual manera esta soportado en todo momento por la alta dirección encargada de la toma de decisiones de alto nivel.

El modelo se fundamenta en las políticas de la organización que ofrece las directrices generales para la planificación del sistema y cumplimiento de objetivos redactados en una forma general sin detalles técnicos. El comité SGSI conformado por la Dirección, Comité de Gestión y Responsable de la Seguridad puede ser complemento del SGC donde ya exista personal que conozca la compañía y que tenga el perfil para la toma de decisiones; este comité se basa en las políticas de la organización para que a partir de ellas se genere un manual de seguridad que será el documento oficial para la descripción de procesos y procedimientos, está encargado de guiar el proceso de certificación en todas sus etapas, autorizados y acompañados por la Dirección para la toma de decisiones. Los procesos son la integración de las diferentes actividades de la organización que permiten obtener un resultado sea un producto o un servicio y según el alcance del sistema se seleccionan aquellos involucrados para aplicar el modelo. Posterior aparecen los procedimientos correspondientes a cada área de la compañía los cuales detallan las actividades que permiten el desarrollo y cumplimiento de los objetivos. Por último la gestión del riesgo son las actividades coordinadas para dirigir y controlar una organización con respecto a la valoración, tratamiento, aceptación y comunicación del riesgo.[34]

[34] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO/IEC 27000 2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2009.

Figura 19: Modelo de gestión propuesto para trabajar el SGSI

Fuente: Los autores.

A.2 ORGANIZACIÓN DE LA SEGURIDAD

Esta fase hace parte de la actividad Establecer el Contexto del flujo gestión del riesgo mostrado en la figura 1 y abarca todos los temas de las cuatro fases de la guía.

A.2.1 Requisito

Análisis y Diagnóstico SGSI.

A.2.2 Acción

Estas acciones acatan además de lo recomendado en ISO/IEC 27005, la gestión de recursos definido en ISO/IEC 27001 capítulo 5: Responsabilidad de la Dirección.

A.2.2.1 Creación grupo SGSI.

Mediante una reunión con los designados, la Dirección declara la adopción del SGSI, específicamente el proceso para la Gestión del Riesgo. Analiza los aspectos organizativos de la Compañía y se conforma el grupo encargado de la organización de la seguridad asignando responsabilidades así:

- Responsable de la Seguridad: Encargado de coordinar la forma de actuar ante incidentes de seguridad.

- Comité de Gestión: Su función es controlar y gestionar las acciones a implementar en el sistema, integrado por personal de diferentes áreas que hacen parte de los procesos bajo gestión.

- Comité de Dirección: Conformados por la Dirección y responsables de tomar las decisiones de alto nivel frente a la seguridad de la información.

A.2.2.2 Plan de Continuidad del Negocio.

De manera opcional la organización puede adoptar el plan de continuidad del negocio (PCN). Hay riesgos imposibles de eliminar ya que no se pueden proteger los activos por completo. La falla de un control implantado o su ineficiencia por selección inadecuada hace que el riesgo residual sobre activos importantes genere consecuencias graves para el negocio llevándolo incluso a detener su producción. Si es considerado, en la misma reunión mencionada en el punto anterior, la Dirección declara la adopción del plan de continuidad del negocio.

La Dirección asigna responsabilidades al grupo SGSI como Comité de Emergencia para desarrollar el plan de acción frente a situaciones críticas o catastróficas, reserva y destina una sala de crisis para su tratamiento hasta encontrar soluciones a corto, mediano y largo plazo que permita recuperar la operación.

A.2.2.3 Realizar acuerdos de confidencialidad.

Dado que personal de mantenimiento y servicios generales contratados directamente por la compañía o tercerizados tienen acceso a las oficinas y archivos donde se celebran las reuniones en las que se tratan temas del negocio de alta confidencialidad, es imperativo realizar con Ellos acuerdos de confidencialidad para proteger la información hablada, procesada y/o almacenada por los grupos SGSI y PCN.

A.2.2.4 Sensibilización y divulgación.

Se inicia un proceso de comunicación hacia toda la organización para crear una cultura de seguridad con el fin de dar a conocer qué se está realizando, ventajas frente al negocio, objetivos, etc. No se revela información confidencial, sino se informa la teoría sobre el SGSI, Gestión del Riesgo y las actividades particulares de la compañía pero en formato general. Esto se puede realizar mediante campañas promotoras internas vía carteleras, intranet, correo electrónico, agenda en comités de área, etc.

A.2.3 Resultados

A.2.3.1 Acta de reunión, firmada por la Dirección y el grupo de organización de la seguridad, donde se evidencia la declaración para adoptar el proceso de Gestión del Riesgo y el y PCN si fue considerado. Se deja evidencia de la creación de dicho grupo definiendo claramente responsables y sus responsabilidades.

A.2.3.2 Acuerdos de confidencialidad firmados con personal de mantenimiento y servicios generales que tiene acceso a las áreas de trabajo del grupo Organización de la Seguridad.

A.2.3.3 Plan de comunicación, sensibilización y divulgación sobre la actividad desarrollada.

A.3 CONTEXTO

Es la primera actividad dentro del proceso de gestión del riesgo ISO/IEC 27005 y corresponde al alcance y límites del mismo y abarca todos los temas de las cuatro fases de la guía. Alineado también con ISO/IEC 27001 4.2.1, esta fase de la guía determina que el propósito del proceso gestión del riesgo es soportar un sistema SGSI, proteger el plan estratégico de la organización, ofrecer conformidad legal, de forma opcional generar un PCN y responder ante incidentes o eventos de seguridad. Mediante estas actividades se definirán los criterios del alcance y límite en este proceso y la organización del mismo, garantizando que todos los activos de información importantes de la compañía sean tomados en cuenta, sin embargo los mismos límites pueden ser causa de riesgos por lo cual deben ser considerados. La guía plantea que dentro del contexto se establecen los criterios que definen todas las actividades del proceso de gestión del riesgo ISO/IEC 27005 y simultáneamente se realiza la primera iteración del ciclo aplicando dichos criterios asignando responsables, responsabilidades y exigiendo la documentación necesaria.

A.3.1 Requisito

- Análisis Diagnóstico SGSI.
- Organización de la Seguridad.

A.3.2 Acción

A.3.2.1 Definir procesos que harán parte de la Gestión del Riesgo.

Esta acción hace parte de la actividad Establecer el Contexto en el proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1. El grupo encargado de la organización de la seguridad de la información consolidará en un documento el

organigrama de la compañía por áreas, consolidará el mapa de procesos con el flujo de actividades respectivo, la interrelación o dependencia entre ellos y el rol responsable de cada uno. También se indicará la tecnología y las sedes físicas/geográficas involucradas. Posteriormente, en reunión documentada en acta, revisará, explicará y entenderá cada proceso enfocándolo con el propósito principal de la compañía o su razón de existencia según el campo de actividad en el mercado, para luego definir cuáles harán parte de la gestión respectiva. Se identificarán aquellos de mayor criticidad para incluirlos en el PCN.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.2 Definir requisitos de seguridad.

Esta acción hace parte de la actividad Establecer el Contexto en el proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1. Estos requisitos de seguridad serán acordes a los objetivos, estructura y necesidades de la organización, por lo tanto es obligatorio conocerla a fondo. Con base en los procesos seleccionados, el rol responsable y el grupo SGSI Gestión del Riesgo establecen con una visión de alto nivel los requisitos de seguridad. Como referencia, en la cuadro 2 se muestra la identificación de estos aspectos. Se identificarán aquellos de mayor criticidad para incluirlos en el PCN.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta

fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

Cuadro 8: Ejemplo requisitos de seguridad para los procesos bajo gestión del riesgo y PCN.

PROCESO	REQUISITO DE SEGURIDAD	ÁREA INTERESADA	MARCO	LEY ASOCIADA	PCN	CONSECUENCIAS
Programa Estratégico	Competitividad.	Dirección	Corporativo	Plan estratégico periodo Y, Misión	SI	Resultados negativos en el negocio.
						Sobrecostos operativos CAPEX-OPEX.
						Sobredimensionamiento infraestructura.
						Deserción de clientes, pérdida de mercado.
						Portafolio de productos insuficiente al cliente.
	Sostenibilidad.	Dirección	Corporativo	Plan estratégico periodo Y, Visión	SI	Resultados negativos en el negocio.
						Sobrecostos operativos CAPEX-OPEX.
						Sobredimensionamiento infraestructura.
						Deserción de clientes, pérdida de mercado.
						Portafolio de productos insuficiente al cliente.
Capacitación	Conservación y actualización del conocimiento, habilidad y experiencia del talento humano.	Gestión Humana	Corporativo	Plan estratégico periodo Y, Misión, Visión	SI	Resultados negativos en el negocio.
						Afectación en Calidad de servicio.
						Pérdida de experticia en diseño e implantación de soluciones.
						Pérdida de mercado.
Comercial	Confidencialidad, Integridad y Disponibilidad de la base de datos de clientes.	Comercial	Corporativo	Política de seguridad	SI	Resultados negativos en el negocio.
						Espionaje industrial.

						Pérdida de mercado.
Comercial	Protección intimidad personal y familiar.	Comercial	Legal	Constitución Política Colombiana, Articulo 15	NO	Demandas. Sobrecostos. Afectación imagen comercial. Pérdida ingresos.
Copias de seguridad y restauración.	Éxito en proceso de copias de seguridad y restauración requerido ante un incidente.	Informática	Corporativo	Política de seguridad	SI	Resultados negativos en el negocio. Interrumpir producción.
Informático.	Protección de la infraestructura informática debido a incendios.	Informática	Corporativo	Política de seguridad	SI	Resultados negativos en el negocio. Interrumpir producción.
Mantenimiento planta física.	Protección de la planta de personal y física por desastres naturales.	Bienes e Inmuebles	Corporativo	Política de seguridad	SI	Resultados negativos en el negocio. Interrumpir producción.
Diseño y Construcción	Cumplimiento acuerdos de nivel de servicio para entrega de bienes y servicios al cliente A.	Producción	Contractual	Contrato de prestación de servicios No xxx	NO	Demandas. Costos. Afectación imagen comercial. Pérdida ingresos.
	Propiedad intelectual en el diseño de soluciones ofrecida a los clientes.	ingeniería	Corporativo	Política de seguridad	SI	Resultados negativos en el negocio. Espionaje industrial. Pérdida de mercado.
Contratación	Cumplimiento de la confidencialidad para el listado de precios relacionado con el suministro de elementos de aseo proveedor A.	Jurídica	Contractual	Contrato de suministro de bienes No xxx	NO	Demandas. Costos. Afectación imagen comercial. Pérdida ingresos.
Pago y cobro de servicios	Autenticidad en las transacciones electrónicas del negocio (No repudio).	Financiera	Corporativo	Política de seguridad	NO	Resultados negativos en el negocio. Demandas. Robo.

a. Marco legal: se debe considerar el marco legal nacional y local sobre seguridad de la información, el marco contractual con clientes, proveedores y propio del negocio para el tratamiento e intercambio de datos a través de tecnologías de información y evitar cualquier delito informático como: protección a la intimidad personal y familiar, transferencia no consentida de activos, hurtos, violación de datos personales, interceptación de datos informáticos, acceso abusivo a sistemas de información, etc. También considerar aquellas de orden socio-cultural. Entre las leyes relacionadas están: Constitución Política Colombiana, manejo de contenidos ilegales a través de la red, ley Estatutaria 1266 del 31 de Diciembre de 2008, circular 052 expedida por la Súper Intendencia Financiera de Colombia que dicta requerimientos mínimos de seguridad para el manejo de información a las entidades que vigila, la ley 527 del 18 de Agosto de 1999 donde se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales, Ley 1273 por medio de la cual se modifica el código penal, comercio y publicidad electrónica, derechos de autor, relación con las administraciones públicas por medios electrónicos, normativa bancaria internacional y otras que apliquen.

b. Análisis de la Misión corporativa: es necesario alinear el propósito y la razón de ser del negocio, el destino de sus resultados y la forma de lograrlos con el proceso de Gestión del Riesgo a definir. En esta instancia será el soporte para las futuras actividades de la guía.

c. Análisis de la Visión corporativa: es necesario alinear el rumbo que permite direccionar decisiones y estrategias de mediano y largo plazo del negocio con el proceso de Gestión del Riesgo a definir. En esta instancia será el soporte para las futuras actividades de la guía.

d. Análisis de Plan Estratégico y Objetivos corporativos: se requiere que la viabilidad del negocio se ajuste a las condiciones del mercado actual por lo tanto es preciso determinar qué estrategias se deben implementar para lograr los objetivos corporativos, esto se logra mediante el plan estratégico. Por lo tanto es requerido alinearlo con los riesgos presentes que amenacen su logro.

e. Análisis de Política de Seguridad: esta contiene las directrices de la seguridad de la información según las necesidades de la organización y la legislación vigente. Son los criterios para proceder ante incidentes de seguridad y asigna funciones y responsabilidades a cada dueño de un proceso, define el alcance

y límite de los activos a proteger. En ella se estipulan los riesgos a los que está expuesta la organización y las medidas de seguridad que se deben tomar. Es única para cada tipo de compañía y debe incluir: la definición de la seguridad de la información y sus objetivos, el alcance de la seguridad de la información y la importancia como mecanismo de control que permite la administración de la información, la declaración por parte de la Dirección apoyando los objetivos y principios de la seguridad de la información, breve explicación de las políticas, definición de responsabilidades generales y especificas en cada rol, no está orientada a personas. Referencia a registros documentales que sustenten la política. Su revisión y actualización es periódica y obligatoria cuando ocurre un incidente o evento de seguridad, ante una auditoria con hallazgos o frente a cambios organizacionales profundos.

f. Comunicación hacia el entorno: es la interfaz formal de la organización hacia sus clientes, proveedores y plano legal, por lo tanto los requisitos de seguridad deben ser consecuentes con lo ofrecido en dichos aspectos, esto incluye la comunicación mediante publicidad, comunicados internos y/o externos, apoyo a proyectos sociales, convenios con entidades públicas o privadas, contratos, etc.

g. Valores de la organización: son los principios o código de conducta que se aplican en el negocio y se promocionan como diferenciador de la competencia. Hace referencia a los acuerdos de niveles de servicio ofrecidos o pactados mediante acuerdos o contratos. Ejemplo: nivel de calidad de un producto/servicio, cumplimiento de especificaciones, etc.

h. Restricciones que afectan la organización: El análisis abarca primero las de orden interno en las cuales se pueden tomar acciones inmediatas, posteriormente aquellas externas cuyo cumplimiento seguramente es obligatorio. Las restricciones sobre los recursos y/o presupuesto de la organización al igual que las de orden operativo, técnico o relacionadas con situaciones críticas como aspectos legales o contractuales que afecten el negocio son las más importantes a considerar. ISO/IEC 27005 considera además las de orden político relacionadas con el gobierno o alguna institución, de carácter territoriales, situación socio económica del país, relacionadas con el programa estratégico, estructurales de la compañía, organizaciones, funcionales, recurso humano laboral, tiempos para implementación por disponibilidad de recursos, tecnológicos (capacidad o limitaciones de redes, hardware, software, licencias), por método, procedimientos o procesos ya

definidos, movidas por un calendario para ajustarse a nuevas leyes o estándares internacionales, culturales, geográficas (ubicación, clima). Pueden existir más pero en conjunto son marco para definir los requisitos de seguridad.

A.3.2.3 Asignar presupuesto.

Esta acción hace parte de la actividad Establecer el Contexto en el proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1. A cargo de la Dirección y apoyada en la definición de requisitos de seguridad, se debe realizar una estimación de alto nivel de los recursos económicos y reservarlos con el fin de implantar y mantener el proceso de Gestión del Riesgo. Este será ajustado a las necesidades durante las iteraciones del proceso y según necesidades de la organización.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.4 Valoración de Riesgos.

Esta acción hace parte de las actividades Establecer el Contexto, Análisis del Riesgo y Evaluación del Riesgo en el proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1. Para los procesos seleccionados, con un enfoque de alto

nivel, como primera iteración del proceso gestión del riesgo y basado en los requisitos de seguridad de la información sustentados por el marco legal, misión, visión, plan estratégico y política de seguridad corporativa, el grupo SGSI y los dueños de los proceso realizan el análisis y evaluación de riesgos a los que se considera está expuesta la organización. Para tal fin se pueden realizar los siguientes pasos:

A.3.2.4.1 Identificación de activos de información. Se debe considerar que un activo es más que software y hardware. La primera tarea que corresponde al dueño de cada proceso seleccionado, apoyado en su grupo de trabajo, consiste en identificar los activos que son clave para el desarrollo de los objetivos del área, esta tarea debe realizarse en un nivel adecuado de detalle la cual se mejora en cada iteración del proceso gestión riesgo. Esta guía utiliza la recomendación ISO/IEC 27005 para agrupar activos pero es posible usar otras como Magerit. ISO/IEC 27005 los clasifica así:

a. Activos Primarios. Se clasifican según:

- Actividades y procesos del negocio: son procesos clave para cumplir la misión, visión de la compañía, que tienen información confidencial o poseen propiedad intelectual.

- Información: datos vitales para la ejecución de los procesos, información personal sensible a protección de intimidad o privacidad, datos estratégicos para cumplir las metas o aquellos cuyo procesamiento y/o almacenamiento implican un alto costo en recurso humano, técnico y financiero.

b. Activos de soporte. Clasificados así:

- Hardware: Son los elementos físicos que dan soporte a los procesos tales como:

  - Equipos de procesamiento de datos fijo (servidores, computadores de escritorio).
  - Equipos de cómputo móvil (computador portátil, asistentes personal digital PDA, celulares).

- Periféricos de procesamiento. Cualquiera conectado a un computador por medio de un puerto de comunicaciones (impresoras, unidades de disco duro removible).
- Medios electrónicos para almacenamiento de datos: Aquellos que se conectan a un computador o una red para almacenamiento de información (CD-ROM, Disco duro removible, memorias USB).
- Medios estáticos o pasivos: Elementos no electrónicos que contienen datos (papel, fax, diapositivas).

- Software: Todos las aplicaciones informáticas que procesan los datos de la organización:

  - Sistema operativo: incluye los programas de los equipos de cómputo que son la base operativa para ejecutar otros programas, servicios o aplicaciones.
  - Software de servicio, mantenimiento o administración: software que complementa los servicios del sistema operativo y no está directamente al servicio de los usuarios ni de las aplicaciones.
  - Paquetes de software o tipo estándar: a diferencia de los desarrollos únicos o específicos, contienen medios, divulgación y mantenimiento, suministran servicios a los usuarios y aplicaciones pero no son personalizados como las aplicaciones del negocio (software para manejo de la base de datos, mensajería electrónica, de grupos, de directorio, para servidor web).
  - Aplicaciones del negocio: Software que brinda a los usuarios acceso directo a servicios y funciones que requieren de su sistema de información (Programa de contabilidad, programas administrativo, gestión de facturación, monitoreo en tiempo real, etc.).

- Red: Dispositivos de telecomunicaciones usados para interconectar equipos de cómputo o sistemas de información separados físicamente y distantes.

  - Medios y soportes: se caracterizan por los rasgos físicos y técnicos del equipo (forma de transmisión, topología) y por los protocolos de comunicación (niveles 2 y 3 del modelo OSI), es decir determina el tipo de red usada (red pública de conmutación telefónica, red local Ethernet o Gigabit-Ethernet, ADSL, acceso inalámbrico WiFi o Bluetooth).
  - Transmisión pasiva o activa: todos los equipos que no son las terminaciones lógicas de las comunicaciones, es decir, son aquellos

dispositivos de soporte de red generalmente propiedad de un proveedor de telecomunicaciones que interconecta las sedes de la organización mediante una red. (enrutadores, radio microondas, modem de fibra o ADSL).
- Interfaz de comunicación: elementos que se conectan a las unidades de procesamiento y se caracterizan por los protocolos empleados (adaptador Ethernet, conversor de interface, modem HSPA).

- Personal: Consiste en todos los grupos de personas que participan en el sistema de información.

  - Personal a cargo de toma de decisiones: son los propietarios de los activos primarios de información y los directores de la organización o de un proyecto específico (Alta dirección, Líder de proyecto).
  - Usuarios: son las personas que manejan los elementos sensibles en las actividades respectivas con responsabilidad sobre tales. Pueden tener permisos especiales de acceso a la información para realizar las labores diarias. (gestión humana, área financiera, gerentes).
  - Personal de operación y mantenimiento: personas a cargo de operación y mantenimiento del sistema de información. Pueden tener permisos especiales de acceso a la información para realizar las labores diarias. (administrador de red y sistema de información, mesa de ayuda, operadores instalación y puesta en servicio).
  - Desarrolladores: son quienes desarrollan las aplicaciones de la organización. Tienen acceso a parte del sistema de información con derechos de usuario de alto nivel pero no toman decisiones sobre los datos de producción. (Ingenieros de desarrollo).

- Sitio: Comprende todos los lugares que contiene el alcance o parte de este y los medios físicos requeridos para su funcionamiento.

  - Ambiente externo: todos los lugares en los cuales no se pueden aplicar los medios de seguridad de la organización. (domicilios del personal, instalaciones de otra organización).
  - Instalaciones: lugar limitado por el perímetro de la organización que está en contacto con el exterior, puede ser una frontera protectora física (edificio, bodega).

- Zona: forma divisiones dentro de una frontera física (oficinas, zonas de acceso reservado).
- Servicios esenciales: todos los servicios que se requieren para que funcione la organización (casino, aseo).
- Comunicación: servicios y equipos provistos por un proveedor de telecomunicaciones. (líneas telefónicas, internet, redes internas).
- Servicios públicos: suministro de energía eléctrica, transformadores, medidores de energía, suministro de agua, medidor de agua, servicio de recolección de residuos, servicio de tratamiento de aguas residuales, servicio purificación de aire, etc.

- Organización: Es la estructura organizacional que contiene todas las áreas y roles del personal asignado a las labores que controlan dicha estructura.

  - Autoridades: organizaciones de las cuales la compañía deriva su autoridad, ellas imponen controles y reglamentos (área administrativa, gestión humana).
  - Estructura de la organización: consiste en las diversas ramas de la organización incluyendo sus actividades transversales bajo el control de las gerencias. (área de sistemas y tecnología, área de compras, unidades de negocios, área de seguridad y vigilancia).
  - Organización del sistema o el proyecto: involucra la organización establecida para un proyecto o servicios específicos (proyecto de desarrollo de una nueva aplicación, proyecto de migración del sistema de información).
  - Subcontratistas, proveedores, fabricantes: entidades que suministran a la organización servicios o recursos regulados mediante contratos. (compañía de instalaciones de abonado, compañía de consultoría, proveedor de personal profesional).

Luego de tener el listado de activos clasificados según la metodología expuesta, el siguiente paso es identificar funciones del grupo de trabajo frente al activo y así determinar el propietario de cada uno y asignarlo como responsable (no necesariamente es quien tiene derechos o toma decisiones importantes sobre el elemento).

Enseguida para cada activo, se clasifican por criticidad en dos aspectos. Primero en función de las consecuencias adversas hacia el proceso en caso de que el activo sufra un incidente o evento de seguridad; en este aspecto los criterios de selección se basan en la reducción hasta la base común del impacto según aspectos a valorar y ordenados por prioridad:

- Incumplimiento de aspectos legales y/o contractuales.
- Interrupción de servicios, alteración de la operación de terceras partes.
- Perdida de confidencialidad, integridad y disponibilidad de la información.
- Afectación de imagen, pérdida de confianza con cliente o proveedores.
- Afectación económica del negocio.
- Seguridad personal y ambiental.
- Crisis: económica, de gobierno, de mercado, orden público, etc.
- Costo de reposición o reparación de los activos

Segundo, basado en las dependencias con otros activos lo cual implica una identificación detallada y documentar tales relaciones. Esto lo hace más crítico para la compañía. Por ejemplo, el hardware y software depende de la infraestructura común como energía y aire acondicionado. Considere una base de datos de clientes del área comercial como un activo de este tipo.
El dueño del proceso y el responsable de cada activo, este último como persona idónea para gestionar todo lo relacionado con el componente, mediante una escala definida asignan su valor de importancia según los criterios definidos en los requisitos de seguridad, el impacto y dependencias analizado en el párrafo anterior. La escala a utilizar es de tipo cuantitativa, en un rango de ***1 a 5 donde 1 es el valor más bajo y 5 el más alto***. De forma opcional, también es importante realizar una valoración por medio de una escala cualitativa que relacione el elemento con un valor en relación a las consecuencias (moneda, indicador, etc.). Para hacerlo se requiere el apoyo de otras áreas como financiera, comercial, contratos, etc. que suministren datos precisos especialmente con cifras.

Es posible que un activo que no tiene dependencia alguna con otro, haga parte de varios procesos en una organización y por lo tanto tenga diferentes valores. En este caso, al activo se le debe asignar el máximo valor de todos y además unificarse para todo el proceso. Para valorar un activo dependiente se aplica la siguiente regla:

- Si el valor del activo dependiente (ej. hardware, software) ≤ valor del activo considerado ➔ Su valor permanece igual.

- Si el valor del activo dependiente (ej. hardware, software) > valor del activo considerado ➔ Su valor se asigna proporcionalmente según el valor de los otros activos y el grado de dependencias.

Por último, la actividad completa debe ser revisada en conjunto con el grupo SGSI para evitar subjetividad y documentar la justificación de selección y criterios de valoración. Se identificaran aquellos de mayor criticidad para incluirlos en el PCN.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

Considere un caso de estudio donde una organización tiene diferentes procesos seleccionados para gestionar el riesgo, entre ellos el proceso Producción en el cual se han identificado y valorado 14 activos, 18 amenazas y 30 vulnerabilidades que conforman 102 escenarios incidentes. Durante el desarrollo de la guía, se irá mostrando cómo se obtuvo cada una de estas cifras. Se obtiene tal cantidad de escenarios incidente debido a que las amenazas y vulnerabilidades se pueden repetir en más de un activo de información, así mismo un solo activo puede estar afectado por diferentes amenazas y vulnerabilidades, finalmente cada combinación individual activo-amenaza-vulnerabilidad es un escenario incidente. Otro sistema, por ejemplo el sistema Financiero tendrá los datos correspondientes a su propio análisis de tal forma que la gestión completa para la organización será la inclusión de todos los sistemas. Para la consolidación de informes es útil el uso

de tablas dinámicas de la aplicación Microsoft Excel. En la figura 4 se muestra como ejemplo la identificación de activos respectiva.

Figura 20: Identificación y valoración de activos proceso de Producción caso de estudio.

Valoración del Activo	Clase de Activo		
Tipo / Activo	PRIMARIO	SOPORTE	Total general
3	2	4	6
HARDWARE		1	1
SERVIDOR DE APLICACIÓN			
INFORMACION	1		1
BASE DE DATOS COMERCIAL			
PROCESOS	1		1
PROCESO GESTION Y SUPERVISION DE CONTRATOS			
PROVEEDORES		1	1
PROVEEDOR DE BIENES Y SERVICIOS			
RED		1	1
RED DE CONECTIVIDAD AVANZADA IP			
SOFTWARE		1	1
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS			
4	1	2	3
INFORMACION	1		1
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS			
PERSONAL TOMA DECISIONES		1	1
LIDER DE PLANEACION			
SERVICIOS PUBLICOS		1	1
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO			
5	3	2	5
ESTRUCTURA ORGANIZACIÓN		1	1
GESTION DE TECNOLOGIA DE LA INFORMACION			
INFORMACION	1		1
PLAN ESTRATEGICO			
INSTALACIONES		1	1
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS			
PROCESOS	2		2
PROCESO APROVISIONAMIENTO DE SERVICIOS			
PROCESO DISEÑO SOFTWARE FINANCIERO			
Total general	6	8	14

A.3.2.4.2 Análisis de estadísticas históricas sobre incidentes o eventos de seguridad. Esta acción hace parte de las actividades Establecer el Contexto y Análisis del Riesgo en el proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1. Con el fin de detectar los riesgos que históricamente ha sufrido la organización, los dueños de los procesos y los responsables de los activos realizan un estudio sobre los incidentes o eventos ocurridos y/o documentados por las compañía durante los últimos cinco años, así como las consecuencias sobrellevadas. De igual manera de acuerdo a la información obtenida se

relacionan los controles existentes organizacionales y técnicos que intervinieron en tales situaciones y se determina un indicador de la eficiencia del mismo como ***Número de incidentes graves anuales ≤ 1***. Para consolidar el informe se cruzan los datos entre procesos y requisitos de seguridad con el inventario de activos. Se deben tener presentes estos resultados para las fases posteriores de la guía con el fin de ajustar o proponer nuevos riesgos y controles según se defina. Luego debe ser revisada con el grupo SGSI gestión del riesgo para plasmar el análisis detectando situaciones de mejora y tener un punto de referencia de acciones preventivas en el proceso de su gestión.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.4.3 Identificación del riesgo: Esta acción hace parte de las actividades Establecer el Contexto y Análisis del Riesgo en el proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1. En esta fase se encuentran, enumeran y se caracterizan los riesgos a los que se considera está expuesta la organización y el propósito es determinar consecuencias o impacto de una pérdida potencial, además de comprender dónde y por qué se origina tal impacto. Dando continuidad al cruce de información entre los procesos, requisitos de seguridad, inventario de activos y referencia sobre incidentes históricos, los dueños de los procesos y los responsables de los activos mediante un enfoque de alto nivel relaciona los posibles riesgos que encuentran hacia estos cumpliendo los siguientes pasos:

a. Identificación de amenazas: Una amenaza es una posible causa de un incidente o evento no deseado que puede resultar en daño a un sistema u organización[35]. Un ejemplo de amenazas son: daño físico, fallas técnicas, terrorismo, espionaje, etc. Para más detalle ver cuadros 3 y 4: Amenazas Comunes y Fuentes de Amenazas Humanas según ISO/IEC 27005 respectivamente.

Cuadro 9: Amenazas Comunes según ISO/IEC 27005.

DOMINIO	AMENAZA INDIVIDUAL
Daño físico	Fuego
	Daño por agua
	Contaminación
	Accidente importante
	Destrucción del equipo
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundación
Perdida de servicios esenciales	Falla en el sistema de suministro de agua o aire acondicionado
	Perdida de suministro de agua
	Falla en el equipo de telecomunicaciones
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales de interferencia comprometedoras
	Espionaje remoto
	Escucha encubierta
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables

[35] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO/IEC 27000 2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2009.

	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Fallas técnicas	Falla del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de los datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Cuadro 10: Fuentes de amenazas humana según ISO/IEC 27005.

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería social • Intrusión, accesos forzados al sistema • Acceso no autorizado al sistema
Criminal de la computación	Destrucción de la información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento (repetición, personificación, interceptación) • Soborno de la información • Suplantación de identidad • Intrusión al sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/terrorismo • Guerra de la información • Ataques contra el sistema (negación del servicio) • Penetración del sistema • Manipulación del sistema

Espionaje industrial (Inteligencia, empresas, gobiernos, extranjeros, otros intereses	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en la privacidad personal • Ingeniería social • Penetración del sistema • Acceso no autorizado al sistema (acceso a información clasificada, de propiedad)
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (error al ingresar datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso (virus, troyano, spam) • Venta de información personal • Errores en el sistema (bugs) • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema

Evidentemente hay más fuentes para identificar las amenazas humanas y deben ser incluidas aquellas que particularmente aplican a la organización, estén o no clasificadas en la referencia anterior. En cualquier caso, se recomienda relacionar las amenazas particulares refiriéndose a los ítems del cuadro. Dichas fuentes pueden ser: organismos industriales, gobierno nacional, compañías de seguros, entidades que realizan estudios de seguridad como por ejemplo: Instituto de Seguridad de Computación de Estados Unidos CSI, Agencia Federal de Investigaciones estadounidense FBI, Grupo Investigativo de Delitos informáticos DIJIN Colombia, S21sec, Panda Security, S21sec, Hispasec Sistemas, Secuware Cybex, Amper, Telefónica, TBSecurity, Barcelona Digital Centro Tecnológico, Universidad de Deusto, Laboratorio S3Lab, Colegio Oficial de Ingenieros de Telecomunicación COIT, etc.

Pueden tener orígenes humanos (requieren especial atención) o naturales, causas accidentales o deliberadas y ser concebidas desde el interior de la compañía o del mundo exterior, ninguna se pasa por alto. Una amenaza puede afectar a varios

activos de información simultáneamente. Tener presente que hay un cambio constante en las amenazas dado el estado del negocio y el entorno por lo cual se considera una revisión periódica según criterio visto más adelante: frecuencia de monitoreo y revisión del contexto, alcance y límite del proceso gestión del riesgo.

Cada propietario de los activos inventariados basado en su criterio y en el histórico de incidentes identifica para cada uno las amenazas encontradas y realiza su valoración utilizando la escala ***Alta, Media o Baja***, en términos de la probabilidad de ocurrencia de acuerdo a la condición de la organización, se documenta la justificación de selección. Luego los resultados obtenidos deben ser revisados en conjunto con el grupo SGSI y los dueños de los procesos para evitar subjetividad.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

En la figura 5 se muestra la identificación de amenazas para el proceso Producción del caso de estudio planteado. Son dieciocho en común pero dado que una afecta varios activos, se conforman treinta y nueve en total.

Figura 21: Identificación y valoración de amenazas proceso Producción caso de estudio.

Valoracion Amenaza / Amenaza / Activo	Cuenta de AMENAZA
Alta	**28**
ABUSO DE DERECHOS	**1**
PROCESO GESTION Y SUPERVISION DE CONTRATOS	
ATAQUES INFORMATICOS	**2**
RED DE CONECTIVIDAD AVANZADA IP	
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	
COMPETENCIA DESLEAL	**2**
BASE DE DATOS COMERCIAL	
PLAN ESTRATEGICO	
DATOS NO CONFIABLES	**4**
LIDER DE PLANEACION	
PROCESO APROVISIONAMIENTO DE SERVICIOS	
PROCESO DISEÑO SOFTWARE FINANCIERO	
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	
ERROR U OMISION	**1**
PROVEEDOR DE BIENES Y SERVICIOS	
ESPIONAJE	**7**
BASE DE DATOS COMERCIAL	
LIDER DE PLANEACION	
PLAN ESTRATEGICO	
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS	
PROCESO APROVISIONAMIENTO DE SERVICIOS	
PROCESO DISEÑO SOFTWARE FINANCIERO	
RED DE CONECTIVIDAD AVANZADA IP	
FALLA EQUIPO	**3**
RED DE CONECTIVIDAD AVANZADA IP	
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO	
SERVIDOR DE APLICACIÓN	
HURTO DCTOS	**2**
PLAN ESTRATEGICO	
PROCESO APROVISIONAMIENTO DE SERVICIOS	
INGENIERIA INVERSA	**1**
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	
INGENIERIA SOCIAL	**4**
GESTION DE TECNOLOGIA DE LA INFORMACION	
PROCESO GESTION Y SUPERVISION DE CONTRATOS	
PROVEEDOR DE BIENES Y SERVICIOS	
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	
PERDIDA SOPORTE	**1**
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS	
Baja	**2**
COPIA ILEGAL SOFTWARE	**1**
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	
EVENTOS NATURALES	**1**
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS	
Media	**9**
ABANDONO DE FUNCIONES	**2**
GESTION DE TECNOLOGIA DE LA INFORMACION	
LIDER DE PLANEACION	
DAÑO FISICO	**1**
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS	
DEFICIENTE SOPORTE PROVEEDOR	**2**
RED DE CONECTIVIDAD AVANZADA IP	
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO	
DESTRUCCION DEL DEQUIPO O LOS MEDIOS	**3**
RED DE CONECTIVIDAD AVANZADA IP	
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO	
SERVIDOR DE APLICACIÓN	
PROCESAMIENTO ILEGAL	**1**
PROCESO APROVISIONAMIENTO DE SERVICIOS	
Total general	**39**

b. Identificación de vulnerabilidades: son las debilidades que padecen los activos o controles y que pueden ser aprovechadas por una o varias amenazas. En términos generales es necesario estudiar las características y propiedades de los activos y controles porque son precisamente lo que se convierte en debilidad cuando no existen o se les saca ventaja de una manera diferente respecto a la función original. Para identificarlas y como referencia ver el cuadro 5 donde ISO/IEC 27005 muestra algunos ejemplos en diversas áreas de seguridad y las amenazas que pueden aprovecharlas.

Cuadro 11: Ejemplos de vulnerabilidades según ISO/IEC 27005

TIPOS	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
Hardware	Mantenimiento insuficiente. Instalación fallida de medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, polvo y suciedad.	Polvo, corrosión, congelamiento.
	Sensibilidad a la radiación electromagnética.	Radiación electromagnética.
	Ausencia de un eficiente control de cambios en la configuración.	Error en el uso.
	Susceptibilidad a las variaciones de voltaje.	Pérdida del suministro de energía.
	Susceptibilidad a las variaciones de temperatura.	Fenómenos meteorológicos.
	Almacenamiento sin protección.	Hurto de medios o documentos.
	Falta de cuidado en la disposición final.	Hurto de medios o documentos.
	Copia no controlada.	Hurto de medios o documentos.
Software	Ausencia o insuficiencia de pruebas de software.	Abuso de los derechos.
	Defectos bien conocidos en el software.	Abuso de los derechos.
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo.	Abuso de los derechos.
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.	Abuso de los derechos.
	Ausencia de pistas de auditoría.	Abuso de los derechos.
	Asignación errada de los derechos de acceso.	Abuso de los derechos.
	Software ampliamente distribuido.	Corrupción de datos.
	En términos de tiempo, utilización de datos errados en los programas de aplicación.	Corrupción de datos.
	Interfaz de usuario compleja.	Error en el uso.
	Ausencia de documentación.	Error en el uso.

	Configuración incorrecta de parámetros.	Error en el uso.
	Fechas incorrectas.	Error en el uso.
	Ausencia de mecanismos de identificación y autentificación de usuario.	Falsificación de derechos.
	Tablas de contraseñas sin protección.	Falsificación de derechos.
	Gestión deficiente de las contraseñas.	Falsificación de derechos.
	Habilitación de servicios innecesarios.	Procesamiento ilegal de datos.
	Software nuevo o inmaduro.	Mal funcionamiento del software.
	Especificaciones incompletas o no claras para los desarrolladores.	Mal funcionamiento del software.
	Ausencia de control de cambios eficaz.	Mal funcionamiento del software.
	Descarga y uso no controlado de software.	Manipulación con software.
	Ausencia de copias de respaldo.	Manipulación con software.
	Ausencia de protección física de la edificación, puertas y ventanas.	Hurto de medios o documentos.
	Falla en la producción de informes de gestión.	Uso no autorizado del equipo.
Red	Ausencia de pruebas de envío o recepción de mensajes.	Negación de acciones.
	Líneas de comunicación sin protección.	Escucha encubierta.
	Trafico sensible sin protección.	Escucha encubierta.
	Conexión deficiente de los cables.	Falla de los equipos de telecomunicaciones.
	Punto único de falla.	Falla de los equipos de telecomunicaciones.
	Ausencia de identificación y autentificación de emisor y receptor.	Falsificación de derechos.
	Arquitectura insegura de la red.	Espionaje remoto.
	Transferencia de contraseñas en claro.	Espionaje remoto.
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento).	Saturación del sistema de información.
	Conexiones de red pública sin protección.	Uso no autorizado del equipo.
Personal	Ausencia del personal.	Incumplimiento en la disponibilidad del personal.
	Procedimientos inadecuados de contratación.	Destrucción de equipos o medios.
	Entrenamiento insuficiente en seguridad.	Error en el uso.
	Uso incorrecto de software y hardware.	Error en el uso.
	Falta de conciencia acerca de la seguridad.	Error en el uso.
	Ausencia de mecanismos de monitoreo.	Procesamiento ilegal de datos.
	Trabajo no supervisado del personal externo o de limpieza.	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.	Uso no autorizado del equipo.
Lugar	Uso inadecuado o descuido del control de acceso físico a las edificaciones y los recintos.	Destrucción de equipos o medios.

	Ubicación en un área susceptible de inundación.	Inundación.
	Red energética inestable.	Pérdida del suministro de energía.
	Ausencia de protección física de la edificación, puertas y ventanas.	Hurto del equipo.
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios.	Abuso de los derechos.
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.	Abuso de los derechos.
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes.	Abuso de los derechos.
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información.	Abuso de los derechos.
	Ausencia de auditorías (supervisiones) regulares.	Abuso de los derechos.
	Ausencia de procedimientos de identificación y valoración de riesgos.	Abuso de los derechos.
	Ausencia de reportes de fallas en los registros de administradores y operadores.	Abuso de los derechos.
	Respuesta inadecuada de mantenimiento del servicio.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimiento de control de cambios.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimiento formal para el control de la documentación del SGSI.	Corrupción de datos.
	Ausencia de procedimiento formal para la supervisión del registro del SGSI.	Corrupción de datos.
	Ausencia de procedimiento formal para la autorización de la información disponible al público.	Datos provenientes de fuentes no confiables.
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información.	Negación de acciones.
	Ausencia de planes de continuidad.	Falla del equipo.
	Ausencia de políticas sobre el uso del correo electrónico.	Error en el uso.
	Ausencia de procedimientos para la introducción del software en los sistemas operativos.	Error en el uso.
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso.
	Ausencia de procedimientos para el manejo de información clasificada.	Error en el uso.
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos.	Error en el uso.
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados.	Procesamiento ilegal de datos.
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información.	Hurto de equipo.

	Ausencia de política formal sobre la utilización de computadores portátiles.	Hurto de equipo.
	Ausencia de control de los activos que se encuentran fuera de las instalaciones.	Hurto de equipo.
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla.	Hurto de medios o documentos.
	Ausencia de autorización de los recursos de procesamiento de la información.	Hurto de medios o documentos.
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad.	Hurto de medios o documentos.
	Ausencia de revisiones regulares por parte de la gerencia.	Uso no autorizado del equipo.
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.	Uso no autorizado del equipo.
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falso o copiado.

También se hace necesario incluir aquellas que particularmente fueron detectadas en la organización y que están o no clasificadas en tal referencia. En todos los casos relacionar las vulnerabilidades particulares refiriéndose a los ítems del cuadro. Otros métodos proactivos involucran software de búsqueda automática de vulnerabilidades el cual analiza la red y aplicaciones que son bien conocidas como vulnerables, por ejemplo el protocolo FPT (File Transfer Protocol) y correo electrónico, sin embargo no tiene en cuenta el entorno y las necesidades de la organización por lo cual los resultados pueden ser imprecisos. Otra forma consiste en realizar una prueba y evaluación controlada de la seguridad donde bajo un plan que determine el funcionamiento y respuesta de los controles se determine las debilidades ocultas. Relacionada con lo anterior, una prueba simulada de acceso no autorizado a los sistemas indica la tolerancia a este incidente o evento de seguridad y permitirá detectar las fallas en los esquemas de protección. Por último la revisión del código del desarrollo de aplicaciones aunque es una medida costosa permite detallar las características desfavorables en seguridad.[36]

Considerar estos criterios: si no se identifica una amenaza no se requiere control aunque sí es necesario identificar y monitorear la vulnerabilidad por su dinámica, una amenaza que no tiene vulnerabilidad asociada puede que no se convierta en riesgo, un control inadecuado o en fallo o su ausencia es una vulnerabilidad. Una amenaza puede tomar ventaja de más de una vulnerabilidad.

[36] NTC-ISO/IEC 27005 Norma Técnica Colombiana. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.

Tener presente que hay un cambio constante en las vulnerabilidades por lo cual se considera una revisión periódica según criterio visto más adelante: frecuencia de monitoreo y revisión del *contexto, alcance y límite del proceso gestión del riesgo*.

Cada propietario de los activos inventariados basado en la metodología descrita, su criterio, experiencia y en el histórico de incidentes identifica para cada activo las vulnerabilidades encontradas y realiza la valoración en una escala ***Alta, Media, Baja***, en términos de los efectos negativos producidos al proceso si una amenaza explota la debilidad del activo. Luego debe ser revisado en conjunto con el grupo SGSI y los dueños de los procesos para evitar subjetividad y donde se documenta la justificación de selección.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

En la figura 6 se muestran las vulnerabilidades identificadas para el caso de estudio planteado relacionadas con las amenazas y activos.

Figura 22: Vulnerabilidades identificadas para el caso de estudio, proceso Producción.

VULNERABILIDAD	Valoracion Vulnerabilidad			
Amenaza / Activo	Alta	Baja	Media	Total general
⊟ALTA CARGA LABORAL			1	1
⊟DATOS NO CONFIABLES			1	1
LIDER DE PLANEACION				
⊟AUSENCIA DE AUDITORIAS EN CUMPLIMIENTO DE PROCESOS	7			7
⊟ESPIONAJE	7			7
BASE DE DATOS COMERCIAL				
LIDER DE PLANEACION				
PLAN ESTRATEGICO				
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS				
PROCESO APROVISIONAMIENTO DE SERVICIOS				
PROCESO DISEÑO SOFTWARE FINANCIERO				
RED DE CONECTIVIDAD AVANZADA IP				
⊟AUSENCIA DE DISPOSICIONES EN LOS CONTRATOS CON EMPLEADOS	4			4
⊟INGENIERIA SOCIAL	4			4
GESTION DE TECNOLOGIA DE LA INFORMACION				
PROCESO GESTION Y SUPERVISION DE CONTRATOS				
PROVEEDOR DE BIENES Y SERVICIOS				
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS				
⊟AUSENCIA DE ESQUEMAS DE REDUNDANCIA EN EQUIPOS Y ENLACE	3			3
⊟ATAQUES INFORMATICOS	1			1
RED DE CONECTIVIDAD AVANZADA IP				
⊟DESTRUCCION DEL DEQUIPO O LOS MEDIOS	1			1
RED DE CONECTIVIDAD AVANZADA IP				
⊟FALLA EQUIPO	1			1
RED DE CONECTIVIDAD AVANZADA IP				
⊟AUSENCIA DE ESQUEMAS DE REEMPLAZOS PERIODICOS		2		2
⊟FALLA EQUIPO		2		2
RED DE CONECTIVIDAD AVANZADA IP				
SERVIDOR DE APLICACIÓN				
⊟AUSENCIA DE MECANISMO DE IDENTIFICACION Y AUTENTIFICACION	10			10
⊟ATAQUES INFORMATICOS	2			2
RED DE CONECTIVIDAD AVANZADA IP				
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS				
⊟ESPIONAJE	7			7
BASE DE DATOS COMERCIAL				
LIDER DE PLANEACION				
PLAN ESTRATEGICO				
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS				
PROCESO APROVISIONAMIENTO DE SERVICIOS				
PROCESO DISEÑO SOFTWARE FINANCIERO				
RED DE CONECTIVIDAD AVANZADA IP				
⊟INGENIERIA INVERSA	1			1
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS				

AUSENCIA DE PROCEDIEMIENTOS MANEJO INFORMACION CLASIFICADA	**10**		**10**
ESPIONAJE	**7**		**7**
BASE DE DATOS COMERCIAL			
LIDER DE PLANEACION			
PLAN ESTRATEGICO			
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS			
PROCESO APROVISIONAMIENTO DE SERVICIOS			
PROCESO DISEÑO SOFTWARE FINANCIERO			
RED DE CONECTIVIDAD AVANZADA IP			
HURTO DCTOS	**2**		**2**
PLAN ESTRATEGICO			
PROCESO APROVISIONAMIENTO DE SERVICIOS			
INGENIERIA INVERSA	**1**		**1**
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS			
AUSENCIA DE PROCEDIMIENTO DE MONITOREO DE LOS RECURSOS DE PROCESAMIENTO	**4**		**4**
ATAQUES INFORMATICOS	**2**		**2**
RED DE CONECTIVIDAD AVANZADA IP			
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS			
DATOS NO CONFIABLES	**2**		**2**
PROCESO APROVISIONAMIENTO DE SERVICIOS			
PROCESO DISEÑO SOFTWARE FINANCIERO			
AUSENCIA DE PROCEDIMIENTOS PARA PRUEBAS EN AMBIENTES SIMULADOS		**2**	**2**
DEFICIENTE SOPORTE PROVEEDOR		**2**	**2**
RED DE CONECTIVIDAD AVANZADA IP			
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO			
AUSENCIA DE PROCESOS DISCIPLINARIOS	**5**		**5**
ABUSO DE DERECHOS	**1**		**1**
PROCESO GESTION Y SUPERVISION DE CONTRATOS			
INGENIERIA SOCIAL	**4**		**4**
GESTION DE TECNOLOGIA DE LA INFORMACION			
PROCESO GESTION Y SUPERVISION DE CONTRATOS			
PROVEEDOR DE BIENES Y SERVICIOS			
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS			
AUSENCIA DE PROCESOS ORIENTADORES SOBRE ASPECTOS ETICOS Y VALORES	**1**		**1**
ABUSO DE DERECHOS	**1**		**1**
PROCESO GESTION Y SUPERVISION DE CONTRATOS			
AUSENCIA DE PROTECCIONES	**3**		**3**
DESTRUCCION DEL DEQUIPO O LOS MEDIOS	**3**		**3**
RED DE CONECTIVIDAD AVANZADA IP			
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO			
SERVIDOR DE APLICACIÓN			
AUSENCIA DE PRUEBAS DE SOFTWARE	**1**		**1**
DATOS NO CONFIABLES	**1**		**1**
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS			
AUSENCIA DISPOSICIONES EN CONTRATOS CON CLIENTES Y TERCEROS	**4**		**4**
DEFICIENTE SOPORTE PROVEEDOR	**2**		**2**
RED DE CONECTIVIDAD AVANZADA IP			
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO			
ERROR U OMISION	**1**		**1**
PROVEEDOR DE BIENES Y SERVICIOS			
PERDIDA SOPORTE	**1**		**1**
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS			

CENTRALIZACION DEL MANEJO DE INFORMACION		2	2
ABANDONO DE FUNCIONES		2	2
GESTION DE TECNOLOGIA DE LA INFORMACION			
LIDER DE PLANEACION			
CONFIGURACION INCORRECTA DE PARAMETROS	2		2
ATAQUES INFORMATICOS	2		2
RED DE CONECTIVIDAD AVANZADA IP			
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS			
DEFICIENCIA EN LA DESCRIPCION DE OFERTA DE SERVICIOS	2		2
COMPETENCIA DESLEAL	2		2
BASE DE DATOS COMERCIAL			
PLAN ESTRATEGICO			
DEFICIENCIA EN PROCESOS COMERCIAL Y MERCADEO	2		2
COMPETENCIA DESLEAL	2		2
BASE DE DATOS COMERCIAL	1		1
PLAN ESTRATEGICO	1		1
DEFICIENCIA EN PROGRAMAS DE BIENESTAR CON LOS EMPLEADOS	4		4
INGENIERIA SOCIAL	4		4
GESTION DE TECNOLOGIA DE LA INFORMACION			
PROCESO GESTION Y SUPERVISION DE CONTRATOS			
PROVEEDOR DE BIENES Y SERVICIOS			
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS			
DESCARGA Y USO NO CONTROLADOS DE SOFTWARE		1	1
COPIA ILEGAL SOFTWARE		1	1
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS			
FALTA DE CONTROL DE ACCESO FISICO	8		8
ESPIONAJE	7		7
BASE DE DATOS COMERCIAL			
LIDER DE PLANEACION			
PLAN ESTRATEGICO			
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS			
PROCESO APROVISIONAMIENTO DE SERVICIOS			
PROCESO DISEÑO SOFTWARE FINANCIERO			
RED DE CONECTIVIDAD AVANZADA IP			
INGENIERIA INVERSA	1		1
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS			
FALTA DE CUIDAD INSTALACION FINAL		3	3
DESTRUCCION DEL DEQUIPO O LOS MEDIOS		3	3
RED DE CONECTIVIDAD AVANZADA IP			
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO			
SERVIDOR DE APLICACIÓN			
FALTA DE MANTENIMIENTO	4		4
DAÑO FISICO	1		1
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS			
FALLA EQUIPO	3		3
RED DE CONECTIVIDAD AVANZADA IP			
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO			
SERVIDOR DE APLICACIÓN			
FALTA DE REDUNDANCIA Y/O ALTERNATIVAS EN PROVEEDORES	1		1
PERDIDA SOPORTE	1		1
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS			

INDISPONIBILIDAD DE RECURSO HUMANO			2	2
ABANDONO DE FUNCIONES			2	2
GESTION DE TECNOLOGIA DE LA INFORMACION				
LIDER DE PLANEACION				
SENSIBILIDAD AL AMBIENTE DE OPERACIÓN			3	3
DESTRUCCION DEL DEQUIPO O LOS MEDIOS			3	3
RED DE CONECTIVIDAD AVANZADA IP				
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO				
SERVIDOR DE APLICACIÓN				
SOFTWARE AMPLIAMENTE DISTRIBUIDO	1			1
COPIA ILEGAL SOFTWARE	1			1
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS				
TRABAJO NO SUPERVISADO	8			8
ABUSO DE DERECHOS	1			1
PROCESO GESTION Y SUPERVISION DE CONTRATOS				
HURTO DCTOS	2			2
PLAN ESTRATEGICO				
PROCESO APROVISIONAMIENTO DE SERVICIOS				
INGENIERIA SOCIAL	4			4
GESTION DE TECNOLOGIA DE LA INFORMACION				
PROCESO GESTION Y SUPERVISION DE CONTRATOS				
PROVEEDOR DE BIENES Y SERVICIOS				
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS				
PROCESAMIENTO ILEGAL	1			1
PROCESO APROVISIONAMIENTO DE SERVICIOS				
UBICACIÓN GEOGRAFICA		1		1
EVENTOS NATURALES		1		1
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS				
USO INCORRECTO HW, SW, PROCEDIEMIENTOS	1			1
DATOS NO CONFIABLES	1			1
LIDER DE PLANEACION				
Total general	85	5	12	102

c. Identificación de consecuencias: las consecuencias son el impacto desfavorable para la organización, el negocio y/o un proceso cuando ocurre un incidente o evento de seguridad, es decir cuando una amenaza saca ventaja de una vulnerabilidad de los activos (escenario incidente). Es el cambio adverso en los resultados de los objetivos planteados, por ejemplo pérdidas económicas del negocio, afectación de la reputación en la marca del producto o servicio, condiciones adversas de operación, etc. Un impacto puede tener diferentes efectos: inmediato sobre el proceso o futuro sobre el negocio, directo con altos costos operativos o indirecto referido a oportunidades, incumplimientos o ganancias perdidas. Aunque el método planteado por la presente guía para estimar y valorar riesgos no requiere identificar y evaluar consecuencias directamente, es importante realizarlo para conocer los escenarios incidentes que podría enfrentar la organización.

Para identificar las consecuencias, se usará la siguiente clasificación genérica y se relacionarán las particulares sentidas para la organización. Ver cuadro 6.

Cuadro 12: Clasificación genérica de consecuencias.

DOMINIO GENÉRICO	IMPACTO PARTICULAR	ACTIVO	VALORACIÓN ACTIVO	ESCENARIO INCIDENTE		VALORACIÓN ESCENARIO
				AMENAZA	VULNERABILIDAD	
Brechas en la seguridad de la información	Perdida de confidencialidad, integridad y disponibilidad.	Base de datos comercial	Crítico (5)	Abuso de los derechos	Falta de proceso de registro y retiro de usuarios	Critico (5)
Degradación de la operación	Altos tiempos de investigación y reparación.	Servidor de aplicación	Crítico (5)	Fuego	Mantenimiento insuficiente	Muy Alto(4)
	Altos costos de reparación.					
	Afectación a salud y seguridad del personal.					
	Afectación de marca, imagen y reputación.					
	Interrupción de servicios.					
Pérdida del negocio en términos técnicos y financieros	Pérdida de liderazgo tecnológico y de mercado.	Formula de producto	Crítico (5)	Espionaje industrial	Trabajo no supervisado de personal externo o aseo	Critico (5)
	Pérdida de clientes o proveedores.					
Alteración de planes, cronogramas	Pérdida de oportunidad.	Líder de proyecto	Muy Alto (4)	Ingeniería social	Ausencia de procedimientos para manejo información confidencial	Muy Alto(4)
	Pérdida de ventaja competitiva.					
	Pérdida de liderazgo tecnológico y de mercado					
Afectación de marca, imagen y reputación	Pérdida de reputación.	Software contable	Medio (3)	Uso de software falso o copiado	Software ampliamente distribuido	Medio (3)
Incumplimientos legales, reglamentarios y/o contractuales	Afectación a terceros.	Proveedor de servicios	Medio (3)	Recuperación de medios reciclados o desechados	Ausencia de procedimiento para el control de cambios y de la documentación.	Medio (3)
	Ataque a la vida privada de usuarios.					
	Procesos judiciales y castigos.					
Impacto en seguridad ambiental, salud y seguridad del personal	Intoxicación del personal	Planta de procesamiento aguas residuales	Muy Alto(4)	Contaminación	Ausencia de reporte de fallas	Muy Alto(4)
	Afectación de fuentes hídricas, fauna y flora.					

El impacto para un proceso debe cuantificarse considerando los escenarios de incidentes empleando los mismos criterios usados para valorar los activos. Para ello se asocian valores del daño en términos cualitativos o cuantitativos, esto requiere el apoyo de otras áreas como financiera, comercial, contratos, etc. que suministren datos precisos especialmente con cifras (moneda o indicador), se recomienda expresarlo en moneda pues facilita la toma de decisiones.[37]
Para la valoración se definen umbrales del impacto y se usará la escala **Alta, Media, baja** que puede combinar ambos aspectos. Para relacionarla con cifras, en moneda por ejemplo: se puede definir que si el costo de la reposición de un activo por daño físico es mayor a COL$10.000.000 es una consecuencia media para un proceso determinado, o si se pierde un negocio debido a competencia desleal que dejaría utilidades por COL$50.000.000 y además afecta la imagen y reputación de la organización es una consecuencia alta. En cualquier caso se debe detallar los valores asociados al impacto y especificar la escala utilizada y los umbrales definidos.

Continuando con la metodología de la guía, cada propietario de los activos inventariados basado en su experiencia, criterio y en el histórico de incidentes, identifica y valora para cada escenario incidente las consecuencias. Luego, el resultado debe ser revisado en conjunto con el grupo SGSI y los dueños de los procesos para evitar subjetividad. Se identificarán aquellas de mayor criticidad para incluirlos en el PCN

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

[37] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO/IEC 27000 2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2009.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

d. Identificación de controles existentes: Los controles son todos aquellos medios utilizados para gestionar el riesgo que permiten llevarlo a niveles aceptables para la organización, incluyen políticas, procedimientos, directrices, prácticas, o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. La finalidad de esta fase es determinar los recursos con los que cuenta la organización para evitar trabajos y costos innecesarios al no duplicar, sobredimensionar o descartar controles. Hasta el momento, el análisis de incidentes históricos permite reconocer los controles existentes y su rendimiento ante el mismo dadas las consecuencias. En esta instancia, aunque continúa el enfoque de alto nivel, se debe complementar para detectar si se requieren nuevas salvaguardas y para ello se cuenta con más información: procesos seleccionados, requisitos de seguridad, presupuesto reservado, inventario de activos, vulnerabilidades, amenazas y consecuencias.

   Por lo anterior, los propietarios de los activos realizan un inventario de controles existentes. Para la identificación es útil tomar referencia de la experiencia propia, planes de tratamiento de riesgo anteriores y realizar visita de validación en sitio. Adicional, es recomendable fijar el estado y grado de funcionamiento de tales controles basado en rutinas de mantenimiento o en auditorías internas o externas al SGSI, para el caso de encontrar un fallo o definir el control obsoleto, corresponde indicar si un control adicional resuelve el inconveniente o definitivamente el control se descarta. De igual manera, considerar los controles planificados a corto plazo logrando evidenciar su real conveniencia. Como en los casos anteriores, luego debe ser revisado en conjunto con el grupo SGSI y los dueños de los procesos para evitar subjetividad y documentar lo propio.

   El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las

necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.4.4. Estimación del Riesgo: Esta acción hace parte de las actividades Establecer el Contexto y Análisis del Riesgo en el proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1. Esta actividad consiste en asignar valores a la probabilidad de ocurrencia y a las consecuencias de un riesgo para estimar su valor en los posibles escenarios de incidentes. Lo anterior indica que la primera acción a realizar es identificar tales escenarios como combinación de las amenazas que explotan una o más vulnerabilidades de uno o más activos y asignar una probabilidad de ocurrencia basado en el criterio de la experiencia propia, estadísticas de la organización y según valoración de criticidad de las variables llevada a cabo en la fase identificación del riesgo. La metodología planteada en la guía busca la mejor relación entre variables y considera escenarios amplios al incluir diversas situaciones, por ello se plantea el uso del método conocido como ***Determinación del valor para la probabilidad y las consecuencias posibles de los riesgos***[38] que se fundamenta principalmente en la importancia de los activos haciendo énfasis en las consecuencias de los escenarios incidentes, además permite realizar un análisis completo de la organización basado en sistemas (procesos o áreas de la compañía) priorizando fácilmente las acciones a seguir entre ellos y a su vez priorizar dentro de cada uno los activos a proteger.

La técnica plantea el siguiente criterio para determinar la probabilidad de los escenarios incidentes:

[38] NTC-ISO/IEC 27005 Norma Técnica Colombiana. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.

Cuadro 13: Criterio para asignar probabilidad del escenario incidente.

Probabilidad de Amenaza	BAJA			MEDIA			ALTA		
Nivel de Vulnerabilidad	B	M	A	B	M	A	B	M	A
Pi escenario	1	2	3	2	3	4	3	4	5

Para facilitar la acción aplicando el método, se continuará haciendo mención al caso de estudio planteado durante el desarrollo del contexto y entretanto en el avance se indicarán las acciones a seguir.

Se debe recordar que para el proceso ***Producción*** se han identificado y valorado 14 activos, 18 amenazas y 30 vulnerabilidades que conforman 102 escenarios incidentes; otro sistema, por ejemplo el sistema ***Financiero***, tendría los datos correspondientes a su propio análisis de tal forma que la gestión completa para la organización será la inclusión de todos los sistemas. Para el ejemplo sólo se trabaja con uno. Es muy útil el uso de tablas dinámicas de la aplicación Microsoft Excel para consolidar, analizar y presentar la información.

Según los datos del sistema Producción, se identifica en la figura 13 que la mayoría de amenazas se repiten en un valor importante sobre un mismo activo (por ello la cuenta muestra 39). Por ejemplo el espionaje es la mayor amenaza y afecta 7 activos relacionados y distribuidos como: uno de tipo Primario-información, tres de tipo Primario-procesos y tres de tipo Soporte. Esto indica que hay un alto impacto de ciertas amenaza sobre la organización en activos específicos y que su efecto es acumulativo, sin embargo el método seleccionado para estimar y valorar el riesgo lo adecúa mediante la probabilidad del escenario que relaciona el nivel de vulnerabilidad, por lo cual en esta instancia no es recomendable implementar controles al respecto.

Como se observa en la figura 6, son varios los activos que tienen la misma vulnerabilidad y que incrementan el número de escenarios incidentes al combinarse con las diferentes amenazas. Los controles a implementar sobre las deficiencias en seguridad que tienen los activos podrán verse reducidos por este aspecto. Por ejemplo implementar el control ***Generar un procedimiento para manejar información clasificada*** se podrá aplicar a 10 activos, tratando así varios riesgos de una vez. Sin embargo como se indicó anteriormente, para tomar

decisiones se requiere un ambiente más amplio que relacione de la mejor forma las variables.

Dado que se tienen identificados y calificados los activos, amenazas y vulnerabilidades es posible obtener la valoración de los escenarios incidentes al aplicar el criterio del cuadro 7 cuyos resultados en relación a los activos se pueden ver en la figura 7. El 83,3% de los escenarios incidentes del proceso producción son los más seguros de sobrevenir (aquellos que tienen probabilidad más alta, es decir 4 y 5) afectando prácticamente todos los activos los cuales están valorados en una importancia media-alta (valores 3, 4 y 5) para la organización.

Figura 23: Cálculo de la Probabilidad de escenarios incidentes caso de estudio.

Valoracion Pi Escenario	Valoracion del Activo			
Activo	3	4	5	Total general
1			**1**	**1**
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS			1	1
2	**2**	**1**		**3**
RED DE CONECTIVIDAD AVANZADA IP	1			1
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO		1		1
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	1			1
3	**7**	**4**	**2**	**13**
GESTION DE TECNOLOGIA DE LA INFORMACION			2	2
LIDER DE PLANEACION		2		2
RED DE CONECTIVIDAD AVANZADA IP	3			3
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO		2		2
SERVIDOR DE APLICACIÓN	3			3
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	1			1
4	**4**	**3**	**2**	**9**
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS			1	1
LIDER DE PLANEACION		1		1
PROCESO APROVISIONAMIENTO DE SERVICIOS			1	1
RED DE CONECTIVIDAD AVANZADA IP	3			3
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO		2		2
SERVIDOR DE APLICACIÓN	1			1
5	**40**	**12**	**24**	**76**
BASE DE DATOS COMERCIAL	6			6
GESTION DE TECNOLOGIA DE LA INFORMACION			4	4
LIDER DE PLANEACION		5		5
PLAN ESTRATEGICO			8	8
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS		6		6
PROCESO APROVISIONAMIENTO DE SERVICIOS			7	7
PROCESO DISEÑO SOFTWARE FINANCIERO			5	5
PROCESO GESTION Y SUPERVISION DE CONTRATOS	7			7
PROVEEDOR DE BIENES Y SERVICIOS	5			5
RED DE CONECTIVIDAD AVANZADA IP	10			10
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO		1		1
SERVIDOR DE APLICACIÓN	1			1
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	11			11
Total general	**53**	**20**	**29**	**102**

Ahora el paso final y concluyente del método en la fase Estimación del Riesgo, con el fin de mantener la relación entre todos los escenarios y establecer el impacto, es definir una nueva variable llamada ***Probabilidad de ocurrencia y criticidad del Riesgo sobre el Activo*** la cual relaciona la valoración de la probabilidad de ocurrencia del escenario incidente con el valor del activo particular. Se determina su escala como baja para valores entre 1 y 3, media para valores

entre 4 y 6 y alta para valores entre 7 y 9, el criterio a utilizar para esta nueva valoración se muestra a continuación:

Cuadro 14: Criterio para determinar la Probabilidad de ocurrencia y criticidad del Riesgo sobre el Activo.

	Valor del activo				
Valor Pi escenario	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**
2	**2**	**3**	**4**	**5**	**6**
3	**3**	**4**	**5**	**6**	**7**
4	**4**	**5**	**6**	**7**	**8**
5	**5**	**6**	**7**	**8**	**9**

Aplicado lo anterior al proceso Producción, el cuadro 9 ofrece una clasificación general para los valores resultantes de la nueva variable resaltando las casillas con los colores: blanco – impacto bajo, amarillo – impacto medio y rojo – impacto alto respectivamente e indicando entre paréntesis la cantidad de escenarios. Para este caso no hay impacto valorado como bajo es decir valores entre 1 y 3.

La figura 8 y el cuadro 9 permiten identificar que el 81,37% de los escenarios tiene consecuencias altas para la organización mientras que solo el 18,63% es de carácter medio, además son los activos primarios como los procesos aquellos que requieren mayor atención. Ahora es más precisa la priorización sobre la gestión del riesgo pero todavía falta medir el efecto acumulativo de varios escenarios sobre un solo activo lo cual se desarrollara en la fase evaluación del riesgo.

Cuadro 15: Probabilidad de ocurrencia y criticidad del Riesgo sobre el Activo caso de estudio.

	Valor del activo				
Valor Pi escenario	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	3	4	5 (1)
2	**2**	**3**	4 (2)	5 (1)	6
3	**3**	**4**	5 (7)	6 (4)	7(2)
4	**4**	**5**	6 (4)	7 (3)	8 (2)
5	**5**	**6**	7 (40)	8 (12)	9 (24)

Figura 24: Estimación del impacto clasificado por activo para el caso de estudio.

Pi Escenario vs Valor Activo	Valoracion del Activo			
Activo	3	4	5	Total general
4	**2**			**2**
RED DE CONECTIVIDAD AVANZADA IP	1			1
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	1			1
5	**7**	**1**	**1**	**9**
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS			1	1
RED DE CONECTIVIDAD AVANZADA IP	3			3
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO		1		1
SERVIDOR DE APLICACIÓN	3			3
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	1			1
6	**4**	**4**		**8**
LIDER DE PLANEACION		2		2
RED DE CONECTIVIDAD AVANZADA IP	3			3
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO		2		2
SERVIDOR DE APLICACIÓN	1			1
7	**40**	**3**	**2**	**45**
BASE DE DATOS COMERCIAL	6			6
GESTION DE TECNOLOGIA DE LA INFORMACION			2	2
LIDER DE PLANEACION		1		1
PROCESO GESTION Y SUPERVISION DE CONTRATOS	7			7
PROVEEDOR DE BIENES Y SERVICIOS	5			5
RED DE CONECTIVIDAD AVANZADA IP	10			10
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO		2		2
SERVIDOR DE APLICACIÓN	1			1
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	11			11
8		**12**	**2**	**14**
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS			1	1
LIDER DE PLANEACION		5		5
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS		6		6
PROCESO APROVISIONAMIENTO DE SERVICIOS			1	1
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO		1		1
9			**24**	**24**
GESTION DE TECNOLOGIA DE LA INFORMACION			4	4
PLAN ESTRATEGICO			8	8
PROCESO APROVISIONAMIENTO DE SERVICIOS			7	7
PROCESO DISEÑO SOFTWARE FINANCIERO			5	5
Total general	**53**	**20**	**29**	**102**

De acuerdo a la metodología anterior, el grupo SGSI y los responsables de los procesos realizan la estimación de riesgo ejecutando dos tareas: adicionan la valoración de los escenarios incidentes a las variables consolidadas en el proceso de identificación de riesgos y lo relacionan con el valor del activo clasificando los riesgos según su criticidad. Se documenta en acta de reunión.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.4.5. Evaluación del Riesgo. Esta acción hace parte de las actividades Establecer el Contexto y Valoración del Riesgo en el proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1. La Evaluación del Riesgo es el proceso de comparar el riesgo estimado contra criterios de clasificación dados para determinar su importancia.[39] De acuerdo a esto la primera labor es para los dueños de los procesos quienes basados en su conocimiento y experiencia determinan dichos niveles con la debida justificación. Se usará la escala bajo, medio y alto. Se pueden apoyar en otras áreas como jurídica, comercial y financiera etc. para sustentarlo, relacionando el impacto hacia la organización de forma cualitativa y/o cuantitativa mediante un indicador funcional o monetario.

Se asignan cuatro tareas al grupo SGSI. La primera y documentado en acta es definir los criterios de clasificación del riesgo basados en las condiciones propias del negocio. Debe asociarse el proceso de estimación de riesgo con umbrales relacionados a un indicador funcional o monetario o a una valoración cualitativa indeterminada y así definir si el riesgo es alto, medio o bajo; también permite especificar el riesgo aceptable por la organización. Por ejemplo, para el proceso de Producción propuesto en el caso de estudio, los cinco riesgos asociados al proceso Diseño de Software financiero en la fase de estimación del riesgo, obtuvieron los máximos valores ya que es un recurso estimado con alta importancia y tienen alta probabilidad de ocurrencia, lo cual será condición para

[39] NTC-ISO/IEC 27005 Norma Técnica Colombiana. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.

declararlos como riesgos altos, sin embargo se debe asociar un umbral para esta decisión lo que finalmente determinará esta valoración. Podría ser que el riesgo es alto si no se logra la meta fijada para la utilidad anual de la compañía al materializarse el robo del código fuente para este desarrollo y/o ceder un 30% del mercado al perder competitividad. En otro escenario, el riesgo de afectación por eventos naturales sobre el edificio y salón de datos es medio dada su probabilidad de ocurrencia, pero si la afectación fue parcial, el umbral definido podrá arrojar un riesgo bajo. Estas relaciones se pueden documentar con los requisitos de seguridad mostrados en el cuadro 2 del apartado A.3.2.2 y la fase estimación del riesgo en A.3.2.4.4.

La segunda tarea para el grupo SGSI es aplicar un filtro a la valoración de riesgos entregada por los dueños de los procesos para evitar subjetividad y reclasificarla si es necesario de acuerdo a los criterios definidos.

La siguiente actividad para el grupo SGSI es priorizar los riesgos sobre los sistemas de la organización (es decir los procesos seleccionados como Producción, Financiero, etc.) y para los activos de cada sistema. Se puede entonces ver la organización como una suma de sistemas, algo así como la ecuación ***Organización = Sistema 1 + Sistema 2 + … + Sistema n.***

Para ello se debe continuar aplicando el método ***Determinación del valor para la probabilidad y las consecuencias posibles de los riesgos*** usado en la fase Estimación del Riesgo, dando un valor de importancia a cada activo dentro del sistema al que pertenece (esta es una valoración diferente a la particular e individual llevada a cabo en la etapa identificación del riesgo y está orientada a definir las prioridades para el posterior tratamiento de los riesgos) y asignando un valor de jerarquía al sistema *n* como la suma de importancia de los activos.

La razón de ser para estas acciones tiene que ver con que cada activo es afectado por varios escenarios incidentes y la nueva valoración debe sumar tales efectos acumulados, es decir, a mayor valor más prioridad. Esta técnica se debe aplicar a cada sistema seleccionado por la organización. En el caso de estudio planteado solo existe Producción.

El cálculo se obtiene al sumar para cada activo de información dentro del Sistema *n* la variable ***Probabilidad de ocurrencia y criticidad del Riesgo sobre el Activo*** (ver A.3.2.4.4. Estimación del Riesgo). Por ejemplo en el caso de estudio para el sistema Producción según la figura 8, el activo ***Proceso de***

Aprovisionamiento de Servicios tiene ocho escenarios incidentes, siete de ellos con probabilidad de ocurrencia y criticidad del Riesgo sobre el Activo con valor 9 y el otro con valor 8. Al aplicar el criterio se obtiene un valor de 71, este determina el nivel de importancia dentro del sistema según comparación con los datos de otros activos. Enseguida se calcula el valor que define la importancia del sistema dentro de la Organización y se calcula sumando todas las importancias de los activos. Como se observa en la figura 17 para Producción se obtiene un valor de 744, entonces el orden de importancia de activos sería Red de conectividad avanzada IP con un puntaje 107, Software de gestión y monitoreo de plataformas con un valor de 86, Plan estratégico con 72 puntos y así sucesivamente. Suponiendo que existe otro sistema llamado Financiero con una puntuación de 900 y con su propio análisis de importancia para sus activos de información. Al final la comparación de estos valores, en orden de mayor a menor, son los que permiten definir las prioridades de atención. Se tratarán primero los sistemas con mayor importancia considerando la misma regla para los activos de información en cada uno.

Figura 25: Importancia de los activos sistema Producción caso de estudio.

Valoración Activo / Activo	Suma de Valor activo vs Pi escenario
⊟3	347
BASE DE DATOS COMERCIAL	42
PROCESO GESTION Y SUPERVISION DE CONTRATOS	49
PROVEEDOR DE BIENES Y SERVICIOS	35
RED DE CONECTIVIDAD AVANZADA IP	107
SERVIDOR DE APLICACIÓN	28
SOFTWARE DE GESTION Y MONITOREO PLATAFORMAS	86
⊟4	146
LIDER DE PLANEACION	59
PLANTILLA DE CONFIGURACION Y ACTUALIZACION DE EQUIPOS PARA SERVICIOS	48
SERVICIOS PUBLICOS AGUA, ENERGIA, TELEFONO	39
⊟5	251
EDIFICIO DE OFICINAS Y SALON DE EQUIPOS DE DATOS	13
GESTION DE TECNOLOGIA DE LA INFORMACION	50
PLAN ESTRATEGICO	72
PROCESO APROVISIONAMIENTO DE SERVICIOS	71
PROCESO DISEÑO SOFTWARE FINANCIERO	45
Total general Sistema Producción	**744**

La última tarea para el grupo SGSI es identificar de acuerdo a la clasificación y priorización realizada, aquellos riesgos de mayor criticidad para incluirlos en el Plan de Continuidad del Negocio – PCN.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.4.6. Plan de Continuidad del Negocio. Esta fase no hace parte del alcance de la norma ISO/IEC 27001 y la presente guía incluye su tratamiento de manera opcional, por lo cual sólo se limita a dar lineamientos generales, sin embargo es muy importante considerar este plan dado que los riesgos no se pueden evitar completamente porque no es posible proteger los activos ante todas las amenazas, de hecho se pueden presentar amenazas nuevas de forma espontánea que no estarán consideradas inmediatamente en la gestión del riesgo. El objetivo general del PCN es definir, implementar y probar el conjunto de procedimientos y estrategias que permitan asegurar la reanudación oportuna y ordenada de los procesos críticos de la organización buscando maximizar el servicio con el mínimo de recursos, de manera que se logre la supervivencia de la organización ante la ocurrencia de un desastre.40 Si se considera la materialización de un riesgo de impacto crítico para una organización que no está preparada, podría afectarla hasta interrumpir sus operaciones, estos son algunos ejemplos[41]:

- Las fallas eléctricas causan el 90% de los incendios. Los problemas más comunes por los que se produce este tipo de siniestros son: la utilización de materiales no adecuados, un cálculo erróneo del sistema o contratar electricistas sin formación técnica.

[40] Plan de divulgación y comunicación VPDRS, ETB S.A. ESP, Abril 2010

[41] INTECO S.A. SGSI en una organización. [En línea] <http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/>[Consultado 25 de Mayo de 2013]

- El 43% de las empresas estadounidenses que sufren un desastre, sin contar con un Plan de Continuidad del Negocio, no se recuperan. El 51% sobrevive pero tarda un promedio de dos años en reinsertarse en el mercado y solo el 6% mantiene su negocio a largo plazo.

- El 30% de las copias de seguridad y el 50% de las restauraciones fallan, según un informe de Enterprise Strategy Group. Durante este estudio muchos departamentos de Tecnología de la Información reconocían no estar seguros de ser capaces de recuperar los datos críticos del negocio y si podrían hacerlo en un tiempo razonable.

Además el PCN debe cumplir unos objetivos específicos:

- Mantener el nivel de servicio en los límites definidos por la compañía y que han sido asumidos por la misma.

- Establecer un periodo de recuperación mínimo para garantizar la continuidad del negocio.

- Recuperar la situación inicial de los servicios y procesos. La recuperación no tiene que ser inmediata y toda al mismo tiempo, ya que puede que existan procesos más críticos que necesiten recuperarse antes.

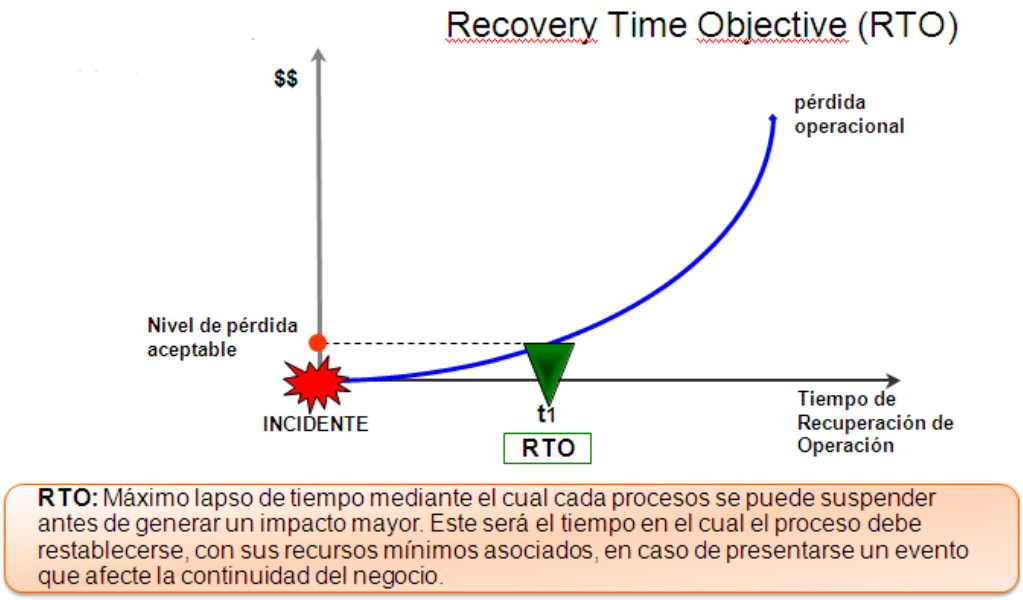
- Analizar el resultado de la aplicación del plan y los motivos del fallo para optimizar las acciones a futuro. Es decir, aprender de las incidencias para mejorar en la respuesta.

Para implementar un PCN se debe cumplir con las siguientes fases:

- Definir el proyecto: objetivos, alcance y política del PCN.

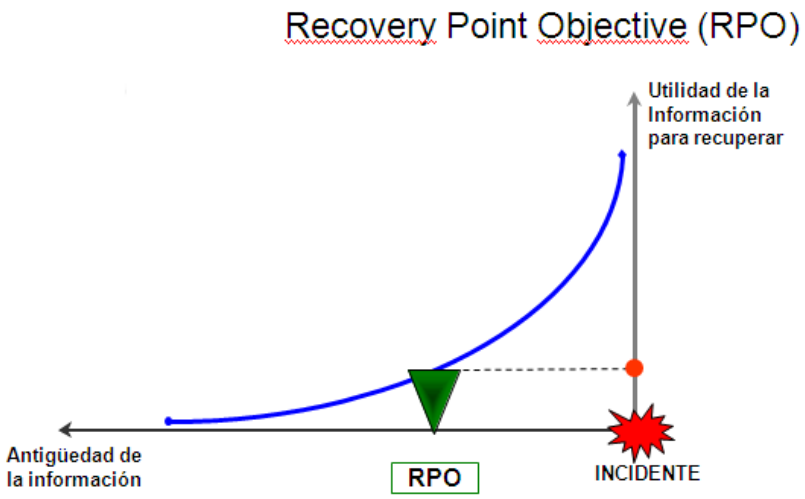
- Valoración de riesgos: fases ya cumplidas en la presente guía. Adicional se debe asignar el tiempo objetivo de recuperación (RTO por sus siglas en ingles) y el punto objetivo de recuperación (RPO).

Figura 26: Definición del Tiempo Objetivo de Recuperación.[42]



[42] Plan de divulgación y comunicación VPDRS, ETB S.A. ESP, Abril 2010

Figura 27: Definición del Punto Objetivo de Recuperación (RPO)[43]



RPO: Máxima perdida tolerable de información para cada uno de los procesos evaluados.

- Diseño del plan de estrategias: se definen los recursos mínimos a nivel económico, técnico y humano entre ellos: grupo de gestión de incidentes, comité de emergencias con un plan de comunicaciones y escalamiento definido y sala de crisis. También se concretan los planes o procedimientos de tratamiento de incidentes y los registros que documenten la situación para su posterior análisis.

- Fase de pruebas, mantenimiento y mejora del PCN: se realiza la prueba inicial y periódica de las estrategias, análisis de resultados determinando el grado de cumplimiento entre tiempo de recuperación actual (RT) y RTO y RPO con el fin de realizar mejoras o actualizaciones al sistema.

- Divulgación, sensibilización y capacitación: el plan debe ser conocido por todo el personal de la organización y practicado por los directos involucrados.

[43] Plan de divulgación y comunicación VPDRS, ETB S.A. ESP, Abril 2010

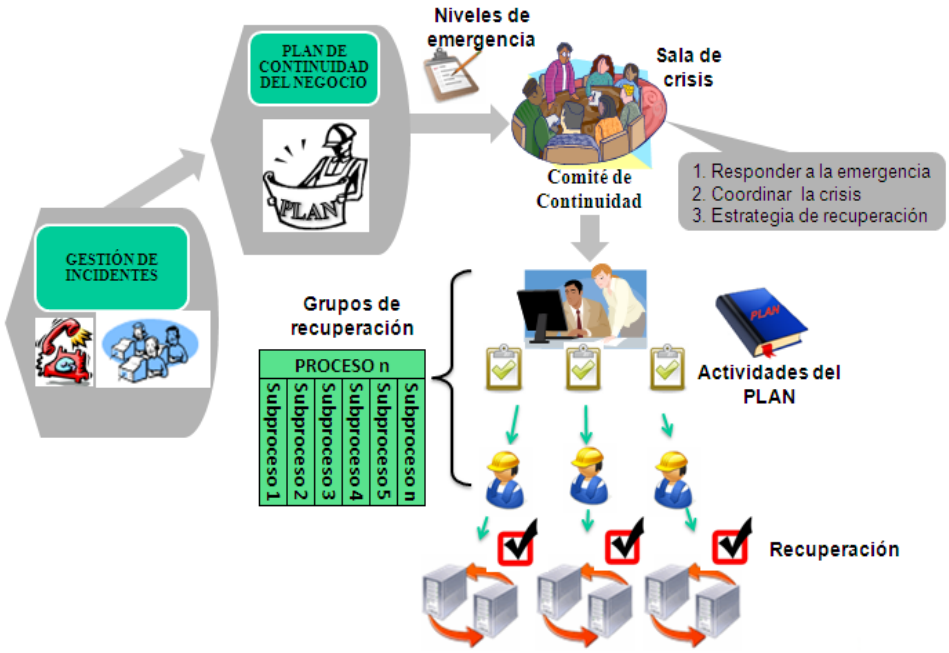
- Documentación final: es el documento que recopila todo el proyecto el cual será consultado por los participantes para seguir los procedimientos y estrategias ante eventos catastróficos.

Figura 28: Planes que componen un PCN.[44]

A continuación se muestran las actividades a seguir luego de un incidente.

Figura 29: Actividades Generales a seguir en un PCN después de un incidente[45].

[44] Plan de divulgación y comunicación VPDRS, ETB S.A. ESP, Abril 2010
[45] Plan de divulgación y comunicación VPDRS, ETB S.A. ESP, Abril 2010



El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.5. Valoración satisfactoria del riesgo.

Es la primera decisión en el flujo de gestión del riesgo mostrado en la figura 14. Si se cuenta con información suficiente para concretar en la siguiente fase las

opciones de tratamiento de los riesgos que permitirán dejarlos en un nivel aceptable para la organización, esta fase será culminada de forma exitosa de lo contrario se hace necesario otra iteración para redefinir el contexto, tener presente que para iniciar el flujo se han tomado decisiones de alto nivel y puede ser que no se cuente con la información detallada al nivel requerido en cuyo caso y bajo decisión de la alta dirección se continuará con las actividades; sólo hasta el ciclo siguiente se podrán redefinir criterios del contexto, tal redefinición también aplicará en caso de otras instancias del proceso para lo cual se harán los ajustes debidos hasta obtener un panorama más claro antes de enfrentar o mejorar las opciones de tratamiento buscando un riesgo aceptable para la organización y en lo posible llevarlo hasta el riesgo residual.

Cabe aquí un análisis a cargo del grupo SGSI de los resultados obtenidos hasta el momento para definir esta etapa. Se hace necesario una reunión del grupo donde mediante acta se documente el análisis y la decisión. En caso de llegar a esta instancia por otras rutas del flujo, se hace necesario un estudio profundo y detallado de las variables dado que hará parte del monitoreo periódico o en el peor de los casos por un incidente o evento de seguridad.

También se define una valoración del riesgo periódica cada 6 meses para actualizar su estado y verificar que sea válido y ajustado a las necesidades de la organización.

De igual forma este análisis será de obligatorio cumplimiento y de forma inmediata cuando ocurran incidentes, eventos de seguridad o cambios en la estructura de la organización, de esta forma se actualizará la gestión frente a la nueva situación del riesgo.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.6. Tratamiento del riesgo.

Esta acción hace parte de las actividades Establecer el Contexto y Tratamiento del Riesgo en el proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1. La guía hasta esta instancia ha permitido clasificar los procesos y activos de información en la organización de acuerdo a los escenarios incidentes presentes y al impacto generado sobre el negocio según los criterios relacionados con los requisitos de seguridad de las partes interesadas, también se han priorizado al asociarlos a una meta organizacional de tal forma que ha sido posible identificar plenamente cuáles son los riesgos altos, medios o bajos para la compañía e incluir los más críticos en un plan de continuidad del negocio.

La siguiente fase de la guía aborda el tratamiento de los riesgos sobre los activos para lo cual se deben implantar medidas para controlar o reducir el impacto sobre ellos cuyo resultado será el riesgo residual que deberá ser analizado por la organización para aceptarlo o no según sus necesidades.

La fase tratamiento del riesgo es vital para la certificación del SGSI. La norma ISO/IEC 27001 en la fase planear capítulo 4.2.1 Establecimiento y Gestión del SGSI aborda en su literal ***c*** la obligación de desarrollar criterios para identificar niveles de riesgo aceptable, en el literal ***e*** determinar el riesgo aceptable o la necesidad de su tratamiento, en el literal ***f*** identificar y evaluar las opciones para el tratamiento de los riesgos, en el literal ***g*** seleccionar los objetivos de control y los controles para el tratamiento de los riesgos, literal ***h*** obtener la aprobación de la dirección sobre los riesgos residuales propuestos y en el literal ***j*** elaborar una declaración de aplicabilidad aprobada por la alta dirección que incluya los objetivos de control y los controles implementados actualmente, los nuevos a implantar y la exclusión de cualquiera de ellos con la debida justificación para su exclusión.

Para escoger la forma de tratar del riesgo, ISO/IEC 27005 define cuatro alternativas no excluyentes entre sí, es decir es posible combinar las acciones para maximizar sus efectos. Ver figura 14:

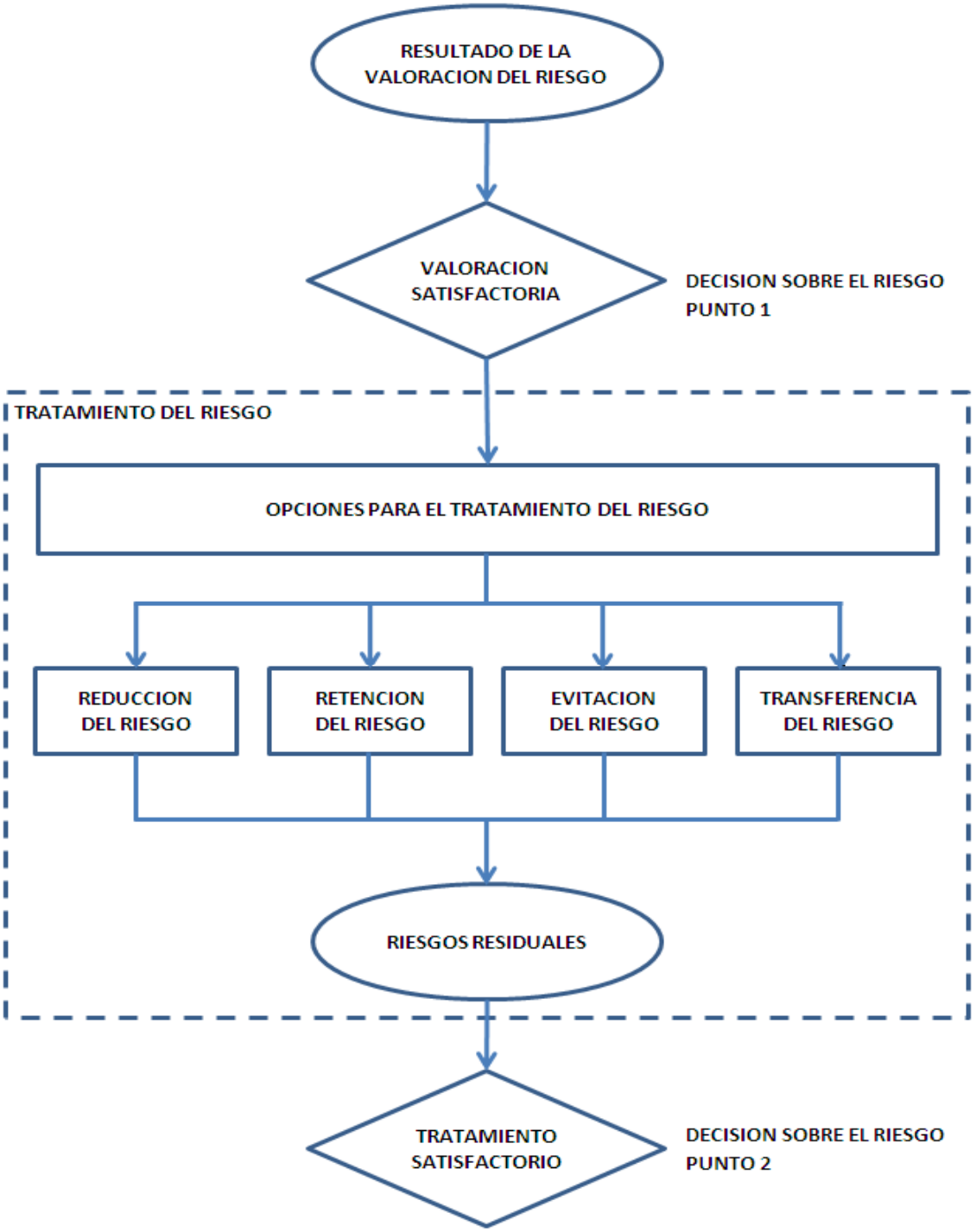
- Reducir el riesgo: Se logra mediante la selección y aplicación de controles con el fin de corregir, eliminar o minimizar un riesgo para proteger un activo.

- Retener el riesgo: No se implementan controles adicionales siempre y cuando el nivel del riesgo esté en niveles aceptables por la organización.

- Evitar el riesgo: Cuando los riesgos y/o los costos de implementación de controles son muy altos se busca evitar la acción amenazante al activo.

- Transferir el riesgo: Se aplica cuando otra área interna o externa puede gestionar mejor el riesgo.

Figura 30: Opciones para tratar el riesgo según ISO/IEC 27005.



Fuente: Proyecto de Norma Técnica Colombiana NTC-ISO/IEC 27001.

Como se indicó anteriormente, luego de aplicar estas opciones para el Tratamiento del Riesgo, queda el riesgo residual el cual es la base de la decisión ***¿Tratamiento Satisfactorio?*** Punto 2 del flujo gestión del riesgo en la figura 14.

Para seleccionar qué medidas aplicar se emplea la metodología de la norma ISO/IEC 27002 la cual cubre la organización mediante 11 dominios o aspectos funcionales de seguridad, 39 objetivos de control que son las metas a cumplir en cada dominio y 133 controles entre organizacionales y técnicos como procedimientos o medidas que contribuyen al cumplimiento de objetivos. La norma además en cada dominio presenta una descripción específica sobre cada objetivo de control y para cada control detalla su significado, muestra una guía de implementación que apoya su puesta en marcha e información adicional que complementa y aclara datos al respecto. A continuación en el cuadro 10 se presenta un resumen de los dominios, objetivos y controles de esta norma.

Cuadro 16: Resumen Dominios, Objetivos de control y Controles ISO/IEC 27002

DOMINIO	OBJETIVO DE CONTROL	CONTROL
5. POLÍTICA DE SEGURIDAD	**5.1 Política de Seguridad de la Información**	5.1.1 Documento de la Política de Seguridad de la Información
		5.1.2 Revisión de la Política de Seguridad de la Información
6.ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN	**6.1 Organización Interna**	6.1.1 Compromiso de la Dirección con la seguridad de la información.
		6.1.2 Coordinación de la seguridad de la información.
		6.1.3 Asignación de Responsabilidades para la Seguridad de la Información
		6.1.4 Proceso de Autorización para los Servicios de Procesamiento de Información.
		6.1.5 Acuerdos sobre Confidencialidad.
		6.1.6 Contacto con las autoridades.
		6.1.7 Contactos con Grupos de Interés Especiales.
		6.1.8 Revisión Independiente de la Seguridad de la Información
	6.2 Partes Externas	6.2.1 Identificación de los Riesgos Relacionados con las Partes Externas.
		6.2.2 Abordaje de la Seguridad cuando se trata con los Clientes.
		6.2.3 Abordaje de la Seguridad en los Acuerdos con Terceras Partes.
7. GESTIÓN DE ACTIVOS	**7.1 Responsabilidad por los Activos.**	7.1.1 Inventario de Activos.
		7.1.2 Propietario de los Activos.
		7.1.3 Uso Aceptable de los Activos.
	7.2 Clasificación de la información.	7.2.1 Directrices de Clasificación.
		7.2.2 Etiquetado y Manejo de la información.
8. SEGURIDAD DE LOS RECURSOS HUMANOS	**8.1 Antes de la Contratación Laboral.**	8.1.1 Roles y Responsabilidades.
		8.1.2 Selección.
		8.1.3 Términos y Condiciones Laborales.
	8.2 Durante la Vigencia del Contrato Laboral.	8.2.1 Responsabilidades de la Dirección.
		8.2.2 Educación, Formación y Concientización sobre la Seguridad de la Información.
		8.2.3 Proceso Disciplinario.
	8.3 Terminación o Cambio del Contrato Laboral.	8.3.1 Responsabilidades en la Terminación.
		8.3.2 Devolución de Activos.
		8.3.3 Retiro de los Derechos de Acceso.
9. SEGURIDAD FÍSICA Y DEL ENTORNO	**9.1 Áreas Seguras.**	9.1.1 Perímetro de Seguridad Física.
		9.1.2 Controles de Acceso físico.

		9.1.3 Seguridad de Oficinas, Recintos e Instalaciones.
		9.1.4 Protección contra Amenazas externas y Ambientales.
		9.1.5 Trabajo en Áreas Seguras.
		9.1.6 Áreas de Carga, Despacho y Acceso Público.
	9.2 Seguridad de los Equipos.	9.2.1 Ubicación y Protección de los Equipos.
		9.2.2 Servicios de suministro.
		9.2.3 Seguridad del Cableado.
		9.2.4 Mantenimiento de los Equipos.
		9.2.5 Seguridad de los Equipos fuera de las Instalaciones.
		9.2.6 Seguridad en la Reutilización o Eliminación de los Equipos.
		9.2.7 Retiro de Activos.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	**10.1 Procedimientos Operacionales y Responsabilidades.**	10.1.1 Documentación de los Procedimientos de Operación.
		10.1.2 Gestión del cambio.
		10.1.3 Distribución (Segregación) de Funciones.
		10.1.4 Separación de las Instalaciones de desarrollo, ensayo y operación.
	10.2 Gestión de la Prestación del Servicio por Terceras Partes.	10.2.1 Prestación del Servicio.
		10.2.2 Monitoreo y Revisión de los Servicios por Terceros.
		10.2.3 Gestión de los Cambios en los Servicios por Terceras Partes.
	10.3 Planificación y Aceptación del Sistema.	10.3.1 Gestión de la Capacidad.
		10.3.2 Aceptación del Sistema.
	10.4 Protección Contra Códigos Maliciosos y Móviles.	10.4.1 Controles contra Códigos Maliciosos.
		10.4.2 Controles contra Códigos Móviles.
	10.5 Respaldo.	10.5.1 Respaldo de la Información.
	10.6 Gestión de Seguridad de las Redes.	10.6.1 Controles de las Redes.
		10.6.2 Seguridad de los Servicios de la Red.
	10.7 Manejo de los Medios.	10.7.1 Gestión de los Medios Removibles.
		10.7.2 Eliminación de los Medios.
		10.7.3 Procedimientos para el Manejo de la Información.
		10.7.4 Seguridad de la Documentación del Sistema.
	10.8 Intercambio de la Información.	10.8.1 Políticas y Procedimientos para el Intercambio de información.
		10.8.2 Acuerdos para el Intercambio.
		10.8.3 Medios Físicos en Tránsito.
		10.8.4 Mensajería Electrónica.
		10.8.5 Sistemas de Información del Negocio.

	10.9 Servicios de Comercio Electrónico.	10.9.1 Comercio Electrónico.
		10.9.2 Transacciones en Línea.
		10.9.3 Información disponible al Público.
	10.10 Monitoreo.	10.10.1 Registros de Auditoría.
		10.10.2 Monitoreo del Uso del Sistema.
		10.10.3 Protección de la Información del Registro.
		10.10.4 Registros del Administrador y del Operador.
		10.10.5 Registro de Fallas.
		10.10.6 Sincronización de Relojes.
11. CONTROL DE ACCESO	**11.1 Requisitos del Negocio para el Control del Acceso.**	11.1.1 Política de Control de Acceso.
	11.2 Gestión del Acceso de Usuarios.	11.2.1 Registro de Usuarios.
		11.2.2 Gestión de Privilegios.
		11.2.3 Gestión de Contraseñas para usuario.
		11.2.4 Revisión de los Derechos de Acceso de los Usuarios.
	11.3 Responsabilidades de los Usuario.	11.3.1 Uso de Contraseñas.
		11.3.2 Equipo de Usuario Desatendido.
		11.3.3 Política de Escritorio Despejado y de Pantalla Despejada.
	11.4 Control del Acceso a las Redes.	11.4.1 Política de Uso de los Servicios en Red.
		11.4.2 Autenticación de Usuarios para Conexiones Externas.
		11.4.3 Identificación de los Equipos en las Redes.
		11.4.4 Protección de los Puertos de Configuración y Diagnostico Remoto.
		11.4.5 Separación en las Redes.
		11.4.6 Control de Conexión a las Redes.
		11.4.7 Control del Enrutamiento en la Red.
	11.5 Control de Acceso al Sistema Operativo.	11.5.1 Procedimientos de Registro de Inicio Seguro.
		11.5.2 Identificación y Autenticación de Usuarios.
		11.5.3 Sistema de Gestión de Contraseñas.
		11.5.4 Uso de las Utilidades del Sistema.
		11.5.5 Tiempo de Inactividad de la Sesión.
		11.5.6 Limitación del Tiempo de Conexión.
	11.6 Control de Acceso a las Aplicaciones y a la Información.	11.6.1 Restricción del Acceso a la Información.
		11.6.2 Aislamiento de Sistemas Sensibles.
	11.7 Computación Móvil y Trabajo	11.7.1 Computación y Comunicaciones Móviles.

	Remoto.	11.7.2 Trabajo Remoto.
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	**12.1 Requisitos de Seguridad de los Sistemas de Información.**	12.1.1 Análisis y Especificación de los Requisitos de Seguridad.
	12.2 Procesamiento correcto en las aplicaciones.	12.2.1 Validación de los Datos de Entrada.
		12.2.2 Control de Procesamiento Interno.
		12.2.3 Integridad del Mensaje.
		12.2.4 Validación de los Datos de Salida.
	12.3 Controles Criptográficos.	12.3.1 Política sobre el Uso de Controles Criptográficos.
		12.3.2 Gestión de Claves.
	12.4 Seguridad de los Archivos de Sistema.	12.4.1 Control del Software Operativo.
		12.4.2 Protección de los Datos de Prueba del Sistema.
		12.4.3 Control de Acceso al Código Fuente de los Programas.
	12.5 Seguridad en los procesos de desarrollo y soporte.	12.5.1 Procedimientos de Control de Cambios.
		12.5.2 Revisión Técnica de las Aplicaciones después de los Cambios en el Sistema Operativo.
		12.5.3 Restricciones en los Cambios a los Paquetes de Software.
		12.5.4 Fuga de Información.
		12.5.5 Desarrollo de Software Contratado Externamente.
	12.6 Gestión de la Vulnerabilidad Técnica.	12.6.1 Control de las Vulnerabilidades Técnicas.
13. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	**13.1 Reporte sobre los Eventos y las Debilidades de la Seguridad de la Información.**	13.1.1 Reporte sobre los Eventos de Seguridad de la Información.
		13.1.2 Reporte sobre las Debilidades en la Seguridad.
	13.2 Gestión de los Incidentes y las Mejoras en la Seguridad de la Información.	13.2.1 Responsabilidades y Procedimientos.
		13.2.2 Aprendizaje Debido a los Incidentes de Seguridad de la Información.
		13.2.3 Recolección de Evidencias.
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**14.1 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.**	14.1.1 Inclusión de la Seguridad de la Información en el Proceso de Gestión de la Continuidad del Negocio.
		14.1.2 Continuidad del Negocio y Evaluación de Riesgos.
		14.1.3 Desarrollo e Implementación de Planes de Continuidad que Incluyan la Seguridad de la Información.
		14.1.4 Estructura para la Planificación de la Continuidad del Negocio.
		14.1.5 Pruebas, Mantenimiento y Reevaluación de los Planes de Continuidad del Negocio.

Fuente: Norma Técnica Colombiana ISO/IEC 27002.

Como primera medida en esta fase de la guía, el grupo SGSI toma el resultado obtenido en la evaluación del riesgo, iniciando con los activos priorizados y clasificados con riesgos altos (contiene aquellos incluidos en el PCN) y sucesivamente en orden de criticidad. Según los requisitos de seguridad afectados y las vulnerabilidades asociadas hace un recorrido de los objetivos de control de la norma buscando la pertinencia de cumplimiento y aplicación de cada uno. El orden a seguir es el mostrado a continuación (esto requiere tener la norma ISO/IEC 27002 a la mano para entender claramente lo que busca cumplir un objetivo particular):

- Dominios que permiten conformar el grupo y directrices de trabajo en SGSI: 5. POLÍTICA DE SEGURIDAD, 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

- Dominios que permitan detectar y reportar eventos o incidentes de seguridad para tomar acciones y recuperar la organización rápidamente ante fallos graves: 13. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN, 14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

- Dominios más sensibles para el negocio: 8. SEGURIDAD DE LOS RECURSOS HUMANOS, 11. CONTROL DE ACCESO, 15. CUMPLIMIENTO.

- Dominios de correcto funcionamiento y seguridad en la prestación del servicio de los sistemas de información: 10. GESTIÓN DE COMUNICACIONES Y OPERACIONES, 12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

- Dominios sobre protección y responsabilidad sobre los activos: 7. GESTIÓN DE ACTIVOS, 9. SEGURIDAD FÍSICA Y DEL ENTORNO

- Objetivos relacionados a directrices propias para cubrir necesidades particulares que no estén incluidos en la norma, estos deberán clasificarse en un dominio afín de la norma para facilitar la trazabilidad.

Si queda algún objetivo sin seleccionar, es obligatorio justificar y documentar las razones. El resultado completo de esta actividad deberá justificarse y

documentarse en una extensión de campos del cuadro 10 manteniendo en ella la relación con los activos.

Hecho lo anterior, cada activo tendrá asociado uno o más objetivos de control que indica la norma, entonces para cada uno el grupo SGSI determinarán los controles que contribuyen al cumplimiento de la meta buscada. Nuevamente se indica la necesidad de contar con la norma ISO/IEC 27002 para entender claramente la descripción del control, su guía de implementación y la información adicional complementaria. Enseguida se aplica la misma acción para los controles particulares (nuevos o existentes) que no necesariamente están identificados en la norma y luego se identifican los controles existentes que ya dispone la organización; tales controles fueron registrados en la fase valoración del riesgo o se podrán tomar en esta instancia, de tal forma que se establece la totalidad de salvaguardas necesarias. Se hará un análisis para determinar el factor común y evitar redundancia en controles, fijar si los existentes cubren las necesidades o requieren actualización para cumplir el fin establecido, el resultado final será el compendio de la mejor alternativa en función de cumplimiento y costo-beneficio. Si queda algún control sin seleccionar, es obligatorio justificar y documentar las razones. El resultado completo de esta actividad deberá justificarse y documentarse en una extensión de campos del cuadro 10 manteniendo en ella la relación con los activos.

Es válida la aplicación de cualquier otra metodología como complemento a esta selección.

La siguiente actividad para el grupo SGSI es considerar las restricciones relacionadas con los controles para realizar un filtro a la selección de estos. Si existen, se debe buscar antecedentes en la organización como apoyo a la decisión de aplicar o no un control basados en las restricciones. Tales limitaciones son[46]:

- Temporales: El control no debe dimensionarse exclusivamente para la vigencia del riesgo o a la vida útil del proceso o activo para el cual fue seleccionado sino que debe aprovecharse al máximo incluso para tratar otros riesgos. Su implantación debe tomar un tiempo razonable y es deseable que sus resultados puedan ser efectivos a un corto plazo.

[46] NTC-ISO/IEC 27005 Norma Técnica Colombiana. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.

- Financieras: Los costos de implantación de un control nunca deben superar el valor del activo. Los costos de operación y mantenimiento inherentes al control proyectados a la vida útil del activo o vigencia del riesgo nunca deben superar el valor del activo. Tampoco podrán ser más costosos que las consecuencias que genera el riesgo. Por último se debe considerar el retorno de la inversión en relación a los beneficios obtenidos por reducir el riesgo. Es recomendable seleccionar los controles considerando lo anterior pero sin restricción de presupuesto, sin embargo en la práctica no siempre es posible equilibrar esta relación por lo cual la alta dirección deberá tomar las decisiones que determinarán el resultado final; esto será considerado más adelante.

- Técnicas: Los controles deben tener una arquitectura física y lógica estándar y abierta no propietaria de tal forma que sea compatible con todos los sistemas, fácilmente actualizable e interoperable con otros controles. Los proveedores deben garantizar la provisión de asistencia técnica y repuestos en hardware y software por un periodo considerablemente largo de tal forma que se pueda tomar ventaja tratando riesgos nuevos que vayan apareciendo a largo plazo.

- Operativas: Un control no puede generar costos excesivos por una operación complicada ya que el mismo control puede inducir al error y no actuar sobre la amenaza, esto incluso puede generar nuevos riesgos. La operación del control no puede requerir mucho personal técnico dedicado a su manejo o generar capacitación costosa de tal forma que el experto sea solo una persona.

- Culturales: Estarán de acuerdo a la región o país donde se implante el control, por ejemplo las requisas a los empleados deberán ser elaboradas por personal del mismo género y esto podría conllevar al incremento en nómina.

- Éticas: También están acorde a la región o país donde se implante el control, de esto dependerá la aplicación de controles que actúan sobre la información que para un empleado puede ser privada, por ejemplo, el análisis del correo electrónico, monitoreo de navegación en internet, relación con personal diplomático, etc.

- Ambientales: Las condiciones climáticas o geográficas del entorno, las leyes gubernamentales sobre este aspecto pueden determinar la viabilidad de un control. Si es pertinente, se recomienda consultar entidades de control para determinar la legislación vigente y realizar o consultar estudios previos sobre el terreno, riesgo de inundación, etc.

- Legales: La legislación vigente en relación al control bajo análisis limitará su selección. Pueden aplicar diferentes aspectos legales según corresponda como son leyes laborales, políticas económicas, seguridad, derechos de autor, protección de datos personales, acuerdos de reserva con terceras partes, la protección del negocio propio en aspectos de integridad, confidencialidad y disponibilidad, etc. Este tema es muy amplio y debe contar con un juicio del área jurídica de la organización o si no existe, de una consultoría externa considerando la necesidad de un acuerdo de confidencialidad.

- Restricciones de personal: La experiencia del personal requerido para administrar un control puede ser muy exigente y no estar disponible en el mercado local o nacional y por lo tanto podría incrementarse la nómina, de tal forma que la implantación del control es inviable. Por otro lado si el personal está disponible en la organización o en el mercado se debe validar que sus competencias, especialmente sus antecedentes, no sean un impedimento para su nombramiento. Se pide apoyar la decisión en las recomendaciones de Gestión Humana y/o de los jefes directos del personal seleccionado.

Ahora el grupo SGSI llevará a cabo un análisis del presupuesto requerido para la implantación de los controles (existentes o planificados) sin ningún tipo de reserva o limite, fijando un periodo anual. Esto requiere realizar cotizaciones con proveedores por bienes y servicios nuevos o por la actualización de aquellos existentes que incluya la capacitación del personal y el mantenimiento periódico requerido. Se deberá asignar un responsable como dueño del control, se resalta la necesidad de seleccionar el personal idóneo con la experiencia técnica y con las competencias necesarias, especialmente sus antecedentes laborales o judiciales. La decisión debe apoyarse en las recomendaciones de Gestión Humana y/o de los jefes directos del personal seleccionado; esto podrá resultar en la necesidad de contratar nuevo personal y por lo tanto afectar el presupuesto. Finalmente se

expondrá ante la alta Dirección para conocer la disponibilidad con que cuenta la organización y se garantizará la reserva en el periodo, así se ajusta frente a lo estimado en el establecimiento del contexto. Si la asignación reduce la cantidad y calidad de los controles, es necesario definir si esto genera nuevos riesgos o modifica los actuales, en caso positivo es seguro que la decisión ***¿Tratamiento satisfactorio?*** en el flujo de gestión del riesgo lleve a una redefinición del contexto, valoración y el mismo tratamiento del riesgo. Esta actividad queda documentada en acta de reunión y se considera como la selección ***definitiva*** de los controles.

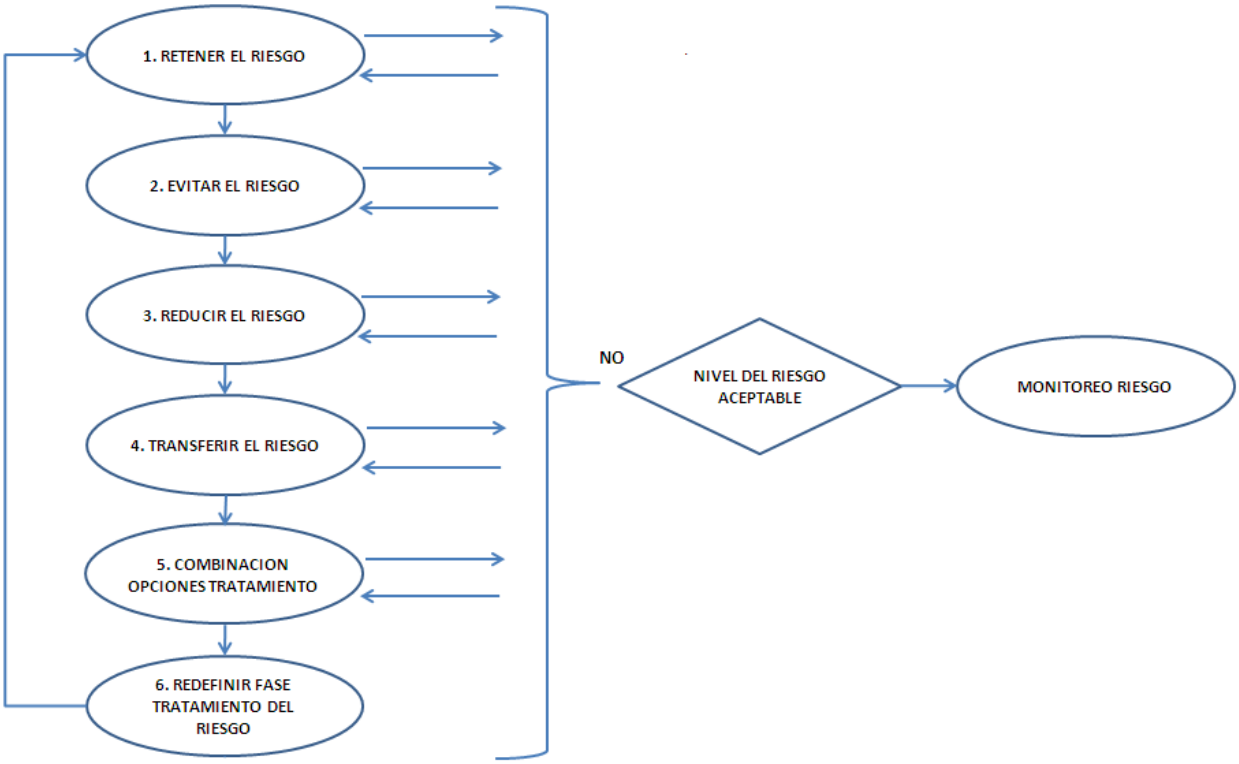
El cruce de objetivos y controles seleccionados mostrará un panorama completo, permitirá visualizar en qué dominios están presentes los activos, si varios activos tienen en común un dominio y si un control protege más de un activo, esto facilita la toma de decisiones al respecto y por ello se ha solicitado documentar la actividad en una extensión de campos del cuadro 10 manteniendo relación con los activos y por lo tanto de los riesgos asociados. El grupo SGSI queda encargado de consolidar esta información, la cual será la Declaración de Aplicabilidad. En el análisis se considerarán todos los objetivos y controles, no se pude obviar ninguno. En este documento quedarán registrados los objetivos de control, controles nuevos, controles existentes, controles particulares y la inclusión o exclusión de cualquiera de ellos con la debida justificación, además deberá ser aprobada por la alta dirección y documentada mediante acta de reunión.

La Declaración de Aplicabilidad resume los resultados que determinan si se pueden asumir o no los riesgos, como también, la disponibilidad y profundidad de la organización para enfrentarlos. A partir de ella y aplicando el procedimiento de la figura 15, el grupo SGSI para un periodo de análisis de resultados definido de 6 meses, planea o proyecta la opción de tratamiento para cada activo en orden de criticidad en función de los escenarios incidentes y el impacto al negocio según la fase evaluación del riesgo, planeando así el riesgo residual proyectado. Esta actividad debe documentarse en acta de reunión donde se evidencie la aprobación de la alta dirección sobre las decisiones tomadas. Se resalta que si antes de finalizar el periodo bajo tratamiento ocurre un incidente con alto impacto para la organización debe revisarse y si es necesario redefinir las fases Contexto, Valoración y Tratamiento del Riesgo en el Proceso Gestión del Riesgo ISO/IEC 27005 mostrado en la figura 1.

Este procedimiento indica que la primera opción a analizar es Retener el Riesgo, si el resultado de esta acción satisface los criterios para aceptarlo se iniciará un

monitoreo del mismo basado en registros que permitan extraer indicadores de eficiencia de los controles asociados. Esta labor será mantenida por el dueño del control durante el periodo de análisis definido. En caso que el nivel del riesgo no sea admisible se continuará bajo el mismo esquema con la siguiente alternativa, es decir Evitar, Reducir, Transferir, o con la combinación de ellas. Si al final no se ha logrado disminuir el impacto del riesgo a lo permitido, se considera redefinir los criterios de aceptación y tratamiento planteados por la organización en esta fase.

Figura 31: Procedimiento inicial para definir la opción de tratamiento del riesgo.



A continuación se detalla cada opción de tratamiento en esta metodología según el orden planteado:

- Retener el Riesgo: Esta actividad es sugerida como la primera opción a tener en cuenta ya que busca aprovechar los recursos que se tienen a mano y racionalizar las inversiones. Se aplica si los controles, actividades o procedimientos actualmente implementados en la compañía sin considerar la acción de los planificados, son suficientes para mantener el riesgo en los

niveles aceptables. Esta acción está considerada en la norma ISO/IEC 27001 en el capítulo 4.2.1 literal ***f*** donde se indica que se deben aceptar los riesgos con conocimiento y objetividad si y sólo si se satisfacen la política y los criterios de la organización.

- Evitar el Riesgo: En línea con el aprovechamiento de recursos y racionalización de inversión, se ha considerado esta como segunda opción en las alternativas de tratamiento; es especialmente útil cuando los riesgos son muy críticos o su tratamiento es muy costoso para un beneficio no significativo. Siempre y cuando no genere nuevos riesgos o produzca un impacto considerable, se busca evitar, reemplazar o modificar la actividad, acción o proceso que sufre el riesgo particular buscando en lo posible alternativas que hagan viable el tratamiento. Esta acción puede implicar una revisión y/o redefinición de todo el proceso de gestión del riesgo.

- Reducir el Riesgo: Esta acción comprende la aplicación de controles para llevar el nivel del riesgo a los niveles deseables para el negocio. Aquí es útil la selección de objetivos de control y controles desarrollada anteriormente y documentada en la declaración de aplicabilidad ya que se consideran adecuados y justificados según el alcance y disponibilidad de la organización, además considera las restricciones que aplican particularmente.

- Transferir el Riesgo: Considerando las restricciones que afectan la selección de controles, si no se afecta la confidencialidad, integridad o disponibilidad de los activos, si no se afecta el negocio y si las opciones anteriores no dan los resultados esperados, el riesgo puede ser transferido a otra área interna o grupo externo que tenga la capacidad de gestionarlo con resultados positivos o que pueda reparar en gran medida las posibles consecuencias que sufra el activo. La acción por sí sola puede generar nuevos riesgos y en caso tal es obligatorio redefinir y actualizar desde el inicio toda la gestión del riesgo realizada hasta ahora, esto será viable siempre y cuando sean mayores los beneficios obtenidos. Es una decisión que compete a la alta dirección ya que son los únicos que pueden influir en la organización para que se transfiera los activos y por tanto los riesgos a otra área o en su defecto aprueben inversiones para subcontratar o adquirir seguros asumiendo si es necesario la actualización de la gestión del riesgo. Es importante aclarar que se puede transferir la responsabilidad para

gestionar el riesgo pero no el impacto generado; los clientes siempre verán como responsable a la organización.

- Combinación de opciones de tratamiento: Como último esfuerzo, se pretende sumar los efectos de las diferentes alternativas de tratamiento. Por ejemplo un riesgo muy alto se puede enfrentar con recursos existentes para rebajar su impacto pero si no se logra el nivel aceptable, como medida adicional se puede contratar un seguro que probablemente será más económico comparado con una protección directa y sin tratamiento alguno.

Retomando, el procedimiento explicado en la figura 15 permite planear el tratamiento del riesgo en un periodo definido y establece el riesgo residual proyectado. También se debe proyectar un monitoreo de los riesgos tratados durante la ejecución de los planes para lo cual es necesario medir la eficiencia de los controles y descubrir el riesgo residual real. Para cumplirlo, el grupo SGSI asigna al dueño de cada control esta responsabilidad, previamente y midiendo el alcance y las restricciones debe divulgarle el resultado de la fase evaluación y tratamiento del riesgo sobre los activos a proteger con el fin de tener juicios para fijar metas e indicadores de rendimiento relacionados con el control.

Fundamentado en lo anterior, el dueño del control definirá un indicador ante eventos individuales y uno global para el periodo de análisis fijando metas de cumplimiento en cada caso. Para ello diseñará un documento donde se registran todos los eventos o incidentes de seguridad presentes sobre el activo protegido y el rendimiento ofrecido por el control. El registro de información será diario documentando incluso si no se presenta ninguna situación. Al respecto se deben considerar variables mínimas como activo protegido, descripción del evento o incidente de seguridad, fecha y hora de ocurrencia, recursos afectados, descripción de la defensa ofrecida por el control, resultado de la contención, cumplimiento de la meta ante el evento individual y de la meta global consolidada. Se incluye dentro de las funciones del dueño del control, cada mes efectuar pruebas de rendimiento a las salvaguardas en ambientes controlados o fuera de línea. También se le asigna la responsabilidad de informar constantemente al grupo SGSI el resultado de la eficiencia del control, especialmente si antes de finalizar el periodo de tratamiento ocurre un evento o incidente de seguridad que no fue contenido satisfactoriamente o si en las pruebas se detectan insuficiencias en el desempeño del control.

El grupo SGSI valida y si es necesario redefine el diseño del registro planteado por el dueño del control, además recopila y analiza los resultados parciales y/o finales de los indicadores de rendimiento de todos los controles. En cada caso la alta dirección aprueba el riesgo residual real obtenido o si no cumple las expectativas de la organización, autoriza revisar o redefinir las fases de gestión del riesgo que sean necesarias.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.7. Tratamiento satisfactorio y aceptación del riesgo.

El tratamiento satisfactorio es la segunda decisión en el flujo de gestión del riesgo mostrado en la figura 1. Aceptación del riesgo es la siguiente etapa luego de la fase tratamiento. La guía hasta esta instancia ha permitido clasificar y priorizar los procesos y activos de información en la organización de acuerdo a los escenarios incidentes, al impacto generado sobre el negocio, a los requisitos de seguridad de las partes interesadas y a las metas estratégicas de tal forma que ha sido posible identificar plenamente cuáles son los riesgos altos, medios o bajos y generar un plan de tratamiento para alcanzar niveles de impacto aceptables por la organización.

En la fase evaluación del riesgo se han establecido criterios para definir el riesgo aceptable y en la fase tratamiento del riesgo de forma sistemática se ha planteado los planes para enfrentarlos, se ha seleccionado los objetivos de control y controles, se ha incluido la aprobación por parte de la alta dirección sobre los riesgos residuales resultantes luego del tratamiento o de la redefinición de fases

del proceso si este no cumple las expectativas de la compañía. De igual forma se han considerado las gestiones necesarias para entregar el insumo requerido por las fases comunicación y monitoreo y revisión del riesgo en el proceso de ISO/IEC 27005. Se ha exigido la justificación y documentación de todas las actividades y toma de decisiones al respecto.

De tal forma que esta acción está casi cumplida, quedaría a cargo del grupo SGSI y la alta dirección complementar y aprobar la documentación respectiva indicando todo lo referente a la aceptación del riesgo y las siguientes acciones a tomar, asumiendo las responsabilidades que todo lo anterior implica, como:

- Cuáles riesgos tratados se han reducido a niveles aceptables y cumplen las expectativas de seguridad de las partes interesadas continuando así con las siguientes fases del proceso.

- Sobre los riesgos tratados pero que se mantienen en niveles intolerables, decidiendo si se debe redefinir solamente la fase de tratamiento o realizar varias iteraciones del ciclo hasta obtener resultados satisfactorio.

- Si se aceptan ciertos riesgos sin tratamiento o tratados pero por encima de niveles aceptables para la organización (por beneficios indirectos o costos de tratamiento demasiado altos) [47] continuando así con las siguientes fases del proceso.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

[47] NTC-ISO/IEC 27005 Norma Técnica Colombiana. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.8. Comunicación del riesgo.

Es la siguiente fase en el proceso de gestión ISO/IEC 27005 luego del tratamiento del riesgo. Se recibe insumo de todas las actividades planteadas en la guía ya que al final de cada una se consideran acciones de comunicación, sensibilización y alineación de planes y decisiones.

El objetivo de la fase es generar un plan de comunicaciones que permita comprensión continua del proceso de gestión del riesgo, además de revisar avances, resultados, alinear y aclarar planes y decisiones entre el grupo SGSI, la alta dirección y los dueños de los procesos[48], estos últimos harán lo propio con su equipo de trabajo particular dando continuidad al plan. No se trata de revisar el desarrollo de actividades puntuales sino de manera gerencial, asegurando que los planes se están realizando como se crearon y con la retroalimentación de todos los involucrados hacer ajustes por rectificaciones o mejoras.

El plan propuesto a desarrollar por el grupo SGSI puede incluir, pero no se limita a las siguientes actividades:

- Cada integrante mide el alcance y las restricciones para divulgar la información sobre el proceso de gestión del riesgo.

- Un comité inicial para revisión general del proceso como punto de partida y en adelante de seguimiento con frecuencia mensual entre los dueños de los procesos y sus equipos de trabajo para desarrollar el objetivo planteado en este capítulo.

- Un comité inicial para revisión general del proceso como punto de partida y en adelante de seguimiento con frecuencia mensual entre el grupo SGSI, la

[48] NTC-ISO/IEC 27005 Norma Técnica Colombiana. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.

alta dirección y los dueños de los procesos para desarrollar el objetivo planteado en este capítulo.

- Consolidar y documentar acuerdos, planes de acción y de mejora.

- Identificar responsables y niveles de escalamiento por las acciones definidas en los nuevos planes.

- Ajustar y documentar conforme a las mejoras identificadas el proceso completo de gestión del riesgo.

- Implementar las acciones acordadas.

- Revisar el avance de implementación de los nuevos planes y del proceso en general.

- El grupo SGSI midiendo el alcance y restricciones resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.9. Monitoreo y revisión del riesgo.

Es la última pero no la menos importante fase del proceso de gestión del riesgo ISO/IEC 27005. En ella convergen el tratamiento y aceptación del riesgo y su resultado puede redefinir o ajustar las demás fases del proceso. Ver figura 1.

Durante la definición de criterios como punto de partida y desarrollo del flujo de gestión del riesgo, la guía oportunamente en cada actividad y no al final del proceso produce insumos y motiva acciones para esta fase canalizando sus resultados en el grupo SGSI. Desde el comienzo se ha considerado un presupuesto inicial que concretado con la organización en la fase tratamiento del riesgo puede llevar a ajustes o redefiniciones de una o más actividades del flujo, lo mismo puede suceder al solicitar una revisión del proceso completo de forma obligatoria cada seis meses o cuando ocurren situaciones importantes como:

- Un incidente o evento de seguridad.

- Cambios en el mapa de procesos.
- Modificación de los requisitos de seguridad.
- Reforma importante en el organigrama de la organización.
- Cambios en la asignación presupuestal para la gestión del riesgo.
- Valoración del riesgo no satisfactoria.
- Tratamiento del riesgo no satisfactorio.

Dado lo anterior, el monitoreo y revisión se justifica por las siguientes razones:

- Se puede modificar la fase identificación de activos ya que pueden aparecer nuevos o es posible que los existentes reciban actualizaciones y por lo tanto la valoración sea diferente.
- Pueden aparecer nuevas amenazas o aquellas ya identificadas cambiar su valoración.
- Lo anterior también sucede con las vulnerabilidades ya que están asociadas a los activos. Vulnerabilidades que antes no tenían una amenaza pueden ser explotadas ante algún cambio del proceso.
- Dado que las amenazas afectan a los activos y estos tienen asociadas las vulnerabilidades, puede cambiar la cantidad de los escenarios incidentes.
- Al modificarse los escenarios incidentes, posiblemente la probabilidad de ocurrencia sea más alta o más baja comparada con la identificación inicial.
- Las consecuencias se mueven acorde a la dinámica de las variables anteriores de tal forma que pueden afectar el negocio de forma diferente a lo inicialmente valorado.
- La fase de estimación del riesgo según corresponda sufrirá cambios importantes.

- La evaluación del riesgo priorizará activos y riesgos de forma diferente.

- Se deberá tomar nuevas decisiones sobre el plan de tratamiento de riesgos.

- Aceptar el riesgo modificado tendrá otras responsabilidades y consecuencias.

En esta instancia también se reciben registros que muestran la eficiencia de los controles implantados según las metas definidas, cuando es necesario los reportes priorizados permiten tomar acciones inmediatas o de lo contrario preparar el proceso para un nuevo periodo de trabajo.

Por otro lado, la metodología definida en la guía para la fase comunicar el riesgo, contribuye considerablemente en esta instancia al permitir una comunicación bidireccional entre quienes toman las decisiones y el equipo de trabajo porque está abierta a recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si aplican los ajustes a la fase tratamiento del riesgo.

En conclusión, las tareas para el grupo SGSI son:

- En apoyo con la alta dirección, identificar los cambios organizacionales importantes como modificación a los procesos y organigrama.

- En apoyo con la alta dirección, identificar cambios relevantes en los requisitos de seguridad y necesidades del negocio.

- En apoyo con la alta dirección, seguimiento al presupuesto proyectado, asignado y a las reservas futuras para el proceso.

- Liderar la revisión del proceso completo de gestión del riesgo ante un cambio organizacional. Redefinir criterios.

- Monitorear periódicamente el avance, novedades y resultados de cada fase del proceso de gestión del riesgo. Soportado en la fase comunicar el riesgo.

- Monitorear los recursos humanos y técnicos de los grupos de trabajo. Soportado en la fase comunicar el riesgo.

- Determinar ajustes necesarios al proceso de gestión del riesgo. Soportado en la fase comunicar el riesgo.

- Analizar registros sobre el desempeño de controles. Soportado en la fase tratamiento del riesgo.

- Analizar las alertas inmediatas entregadas por los propietarios de los controles sobre incidentes de seguridad o eventos no controlados adecuadamente.

- Liderar la revisión del proceso completo de gestión del riesgo ante un incidente o evento de seguridad no controlado adecuadamente. Redefinir criterios.

- Seguimiento y análisis de resultados a los cambios y ajustes implementados.

- Liderar la revisión periódica y preventiva cada 6 meses del proceso completo de gestión del riesgo. Redefinir criterios.

- Definir acciones y tomar decisiones ante cualquier situación.

- Documentar todas las acciones y decisiones tomadas en esta actividad.

- Actualizar el plan de cultura de seguridad organizacional iniciado en la fase organización de la seguridad apartado A.2.2.4 donde se realiza divulgación, sensibilización y comunicación hacia todos los colaboradores de la empresa.

El grupo SGSI se asegura de sensibilizar, comunicar y formalizar las decisiones tomadas y los resultados obtenidos a las personas o grupos involucrados en esta fase. Es necesario evidenciar que los líderes de grupo o jefes inmediatos hagan lo propio con su equipo de trabajo para que los planes tengan continuidad. De igual forma se permite recibir de las partes interesadas todas las observaciones y recomendaciones al respecto y bajo análisis del grupo SGSI se determinará si

aplican los ajustes a la fase tratamiento del riesgo buscando cubrir las necesidades pertinentes de seguridad de la información. Es útil realizar comités particulares con los grupos que hacen parte de esta fase. Posteriormente todas las actividades aquí descritas como las decisiones finales deben quedar documentadas en actas de reunión.

Por último, el grupo SGSI midiendo el alcance y restricciones, resume información básica según criterios y decisiones tomadas en esta fase, se apoya en el área de comunicaciones para alimentar el plan de comunicación y sensibilización dirigido a toda la organización y definido en el apartado A.3.2.10.

A.3.2.10. Plan de comunicación y divulgación.

Se continúa con el plan de comunicación hacia toda la organización para crear una cultura de seguridad con el fin de dar a conocer qué se está realizando, ventajas frente al negocio, objetivos, etc. En esta instancia se realiza de acuerdo a los criterios definidos y decisiones tomadas en las acciones para definir el contexto y para realizar la implantación del proceso de gestión del riesgo en el apartado A.3 a saber: inclusión de procesos a gestionar, definición de requisitos de seguridad, valoración, tratamiento, aceptación, comunicación y monitoreo de riesgos.

Este plan recibe insumo por parte del SGSI por cada fase del proceso.

No se revela información confidencial, sino que se informa la teoría sobre el SGSI - Gestión del Riesgo y las actividades particulares de la compañía pero en formato general. El grupo SGSI con el apoyo de las áreas de comunicación de la compañía realizan esta labor mediante campañas promotoras internas vía carteleras, intranet, correo electrónico, agenda en comités de área, etc. Se documentan todas las acciones tomadas al respecto en la carpeta del plan.

A.3.3 Resultados

A.3.3.1. Acta de reunión del grupo SGSI donde se documentan los procesos seleccionados para gestionarles el riesgo, producto del primer fuljo de la gestión o de una actualización del sistema. Se identifica la relación entre ellos y en cada caso se detalla el flujo de actividades. Si la organización lo ha considerado se

deben incluir en el PCN los de mayor criticidad. Se asignan responsables para cada proceso. Se justifican aquellos excluidos por la organización.

A.3.3.2. Acta de reunión, evidencia sobre los requisitos de seguridad consolidados para los procesos seleccionados en la gestión del riesgo producto del primer fuljo de la gestión o de una actualización del sistema, considerando el marco legal, misión, visión, objetivos corporativos, planes estratégicos, política de seguridad y comunicación hacia el entorno corporativo. Si aplica, se identifican cuáles necesidades de las partes interesadas harán parte del PCN.

A.3.3.3. Presupuesto requerido para el proceso de Gestión del Riesgo. Acta de reunión entre el grupo SGSI y la alta dirección donde se planean y reservan los recursos económicos iniciales con el fin de implantar el proceso de Gestión del Riesgo. En esta carpeta también reposarán los ajustes presupuestales aprobados según las necesidades de la organización durante las iteraciones del flujo para mantener el proceso.

A.3.3.4. Relacionando los procesos y requisitos de seguridad seleccionados y manteniendo la correspondencia con las variables que en adelante aparecen, un registro aprobado por el grupo SGSI en el cual se documenta de manera formal el resultado final o una actualización de la valoración de riesgos comprendida por el análisis y evaluación de riesgos. Así, este documento debe incluir:

i) Inventario de activos. Clasificados por las categorías según ISO/IEC 27005 y a la prioridad asignada, valorados de acuerdo a la escala definida relacionando el impacto hacia la organización, se identifican aquellos que harán parte del PCN. Se identifica el dueño del activo y se asigna como su responsable en adelante.

ii) Consolidado de incidentes o eventos de seguridad durante los últimos 5 años. Se identifican los controles existentes que intervinieron en la contención de los riesgos determinando su eficiencia y se calculan las consecuencias sobrellevadas por la organización. Se documentan los planes de tratamiento implementados.

iii) Análisis del Riesgo.

a. Inventario de amenazas. Valoradas según la escala definida, clasificadas por dominio y fuente según ISO/IEC 27005, incorporando aquellas detectadas por un origen diferente a esta metodología.

b. Identificación de vulnerabilidades. Una lista de vulnerabilidades clasificadas según parámetros de ISO/IEC 27005 incluyendo las detectadas por otras fuentes, valoradas según la escala definida. Se debe documentar cuáles carecen de control o presentan fallos, además se debe resaltar aquellos grupos de vulnerabilidades que tienen amenazas comunes, las que no tienen amenazas asociadas y viceversa con el fin de establecer un monitoreo constante.

c. Identificación de consecuencias. Para cada escenario incidente, la identificación y valoración de consecuencias clasificadas por dominio ISO/IEC 27005 y por la escala definida respectivamente, registrando el costo del impacto en forma cuantitativa o cualitativa, sea por moneda o indicador organizacional. De igual forma determinar las consecuencias a incluir en el PCN.

d. Identificación de controles existentes. El inventario de controles existentes clasificado y referido al proceso que pertenece, determinando su grado de funcionamiento según la fuente que define dicho estado. También relacionando aquellos controles que se descartan por fallos u obsolescencia. Se deben incluir los controles planificados a corto y mediano plazo de cada proceso que no están en producción como también aquellos considerados como nueva opción.

iv) Estimación del riesgo. Una lista de activos de información y riesgos con valor asignado según el método definido en la guía el cual está basado en la identificación de los escenarios incidentes, la probabilidad de ocurrencia y la importancia de los activos. Se identifican amenazas y vulnerabilidades comunes a estos.

v) Evaluación del riesgo. Una lista riesgos clasificados y valorados según la escala definida relacionando el criterio de asignación de forma cuantitativa o cualitativa según un valor monetario o indicador organizacional. De igual forma una lista de procesos priorizados en la compañía para gestión del riesgo y una

lista de activos priorizados dentro de cada proceso. Se identifican aquellos de mayor criticidad a incluir en el PCN.

vi) Plan de continuidad del negocio. Si la organización ha determinado implementarlo, el resultado es el documento donde se define el plan de continuidad del negocio según los fundamentos ofrecidos en la guía.

A.3.3.5. Valoración satisfactoria del riesgo. Acta de reunión aprobada por el grupo SGSI y la alta dirección donde se documenta que la actividad de valoración de riesgos ha suministrado información suficiente, cubre las necesidades de la organización y por lo tanto es exitosa y así es posible continuar con las siguientes actividades del proceso gestión del riesgo. En caso contrario, el acta debe registrar las decisiones tomadas para redefinir parte o todas las actividades previas hasta obtener resultados favorables para la compañía.

A.3.3.6. Tratamiento del riesgo. Plan de tratamiento de riesgos aprobado por la alta dirección. La carpeta mediante las actas de reunión exigidas debe evidenciar las decisiones tomadas para aplicar el plan a los riesgos identificados, valorados y priorizados según la metodología planteada en la guía. Debe contener la declaración de aplicabilidad dando trazabilidad a la selección de objetivos de control y controles según las restricciones detectadas, identificar el riesgo residual proyectado para el periodo de análisis y ante un evento o incidente de seguridad no tratado adecuadamente, identificar a los responsables de los controles y consolidar los entregables como indicadores y reportes que este rol debe pasar al grupo SGSI para análisis en la fase monitoreo del riesgo. También se documentan todos los ajustes realizados al proceso movidos por los comités para desarrollar la comunicación del riesgo y los insumos para el plan de comunicación y sensibilización corporativo.

A.3.3.7. Tratamiento satisfactorio del riesgo. Acta de reunión aprobada por el grupo SGSI y la alta dirección evidenciando las decisiones referentes a la aceptación del riesgo y las siguientes acciones a tomar, asumiendo las responsabilidades que todo lo anterior implica. Este documento debe indicar los riesgos que se han reducido a niveles aceptables y admitidos por la organización, se listan aquellos riesgos tratados cuyo nivel es intolerable y no se aceptan, también se incluyen aquellos riesgos tratados o no que la compañía admite por

encima de niveles admisibles movida por beneficios indirectos o costos de tratamiento demasiado altos. En cada caso se indica si se continúa con las siguientes fases del proceso o se redefinen actividades del proceso de gestión del riesgo.

A.3.3.8 Comunicación del riesgo. Con los reportes obtenidos en cada actividad del proceso gestión del riesgo, las actas de comité realizadas entre la alta dirección, el grupo SGSI y los dueños de los procesos donde se evidencie seguimiento, cumplimiento, aclaración y alineación de conceptos conforme a las decisiones tomadas frente al proceso, revisión de avances y resultados de cada fase y ajustes dados por rectificaciones o mejoras sugeridas por las partes interesadas.

A.3.3.9 Monitoreo y revisión del riesgo. Con la información consolidada por el grupo SGSI durante las fases valoración y tratamiento de riesgos, registros con evidencias por el seguimiento y ajustes al proceso de gestión del riesgo. Tales arreglos pueden ser al presupuesto requerido por el sistema, revisiones o redefiniciones de algunas actividades o del proceso completo motivadas por incidentes o eventos de seguridad, cambios en mapas de procesos, cambios en el organigrama de la compañía o simplemente por el fin de la vigencia del periodo en análisis, como también por una valoración o tratamiento de riesgos no satisfactoria y debido a los resultados de la fase comunicación del riesgo.

A.3.3.10. Plan de comunicación, sensibilización y divulgación sobre las actividad desarrolladas.

Bibliografía

ETB S.A. E.S.P. (2010). *Plan de Comunicación y Divulgación VPDRS.* Bogotá.

ICONTEC. (2006). *Norma Técnica Colombiana NTC-ISO/IEC 27001 - Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.* Bogotá: ICONTEC.

ICONTEC. (2009). *NTC-ISO/IEC 27005 Norma Técnica Colombiana. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.* Bogotá: ICONTEC.

INTECO S.A. (25 de Mayo de 2013). *SGSI en una organización.* Obtenido de http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2009). *ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Suiza.