ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DESARROLLO DE UN PLAN DE RIESGOS DE SEGURIDAD PARA EL PROCESO DE EMISIÓN DE PÓLIZAS PARA UNA EMPRESA DE SEGUROS DEL ECUADOR, SIGUIENDO LA NORMA ISO 27001:2013"

TESIS DE GRADO

Previa la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Jenny Margarita Garzón Balcázar

GUAYAQUIL – ECUADOR

AÑO

2.016

AGRADECIMIENTO

Agradezco a Dios por todas las bendiciones recibidas, por su constante compañía y por su amor infinito.

A mi padre que está en el cielo por heredarme su fortaleza, espíritu de lucha y perseverancia. A mi madre por su valentía frente a la vida, por su constancia, su amor incondicional y por estar presente en cada paso de mi vida.

A mi esposo por su amor, paciencia y solidaridad.

A mi familia por su calor fraterno y por ser el pilar fundamental en mi vida.

A mi tutor por su paciencia y apoyo para la culminación de este proyecto.

DEDICATORIA

A Dios, a mis padres, a mi esposo, a mis hijos, a mi familia, tutor, maestros y amigos y a todos aquellos que estuvieron conmigo.

TRIBUNAL DE SUSTENTACIÓN

DIRECTOR MSIG/MSIA

ING. LENÍN FREIRE

DIRECTOR DEL PROYECTO DE GRADUACIÓN

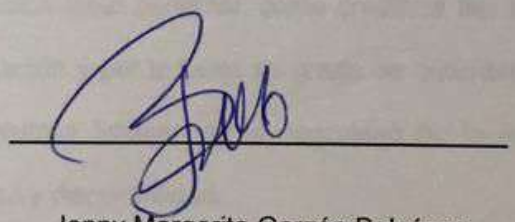
ING. LENÍN FREIRE

MIEMBRO DEL TRIBUNAL

ING. ROBERT ANDRADE

DECLARACIÓN EXPRESA

"Declaro de forma expresa que todo el contenido de esta Tesis de Grado es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"



Jenny Margarita Garzón Balcázar

RESUMEN

Desarrollar un plan de riesgos de seguridad para el proceso de emisión de pólizas basado en la norma ISO 27001:2013, norma que define las acciones para lograr dicho objetivo. El uso de este esquema permitirá evaluar de manera adecuada los riesgos en referencia a los activos de información, de tal forma que se puedan establecer controles y realizar la valoración necesaria para contrarrestar las vulnerabilidades y amenazas y con ello mejorar la eficacia y eficiencia de la empresa aseguradora.

Al tener la póliza información tanto personal, como crediticia del cliente, se convierte en el principal activo de información y por lo tanto su grado de criticidad es alto por lo que debe cumplir con las características básicas de la seguridad de la información como son: la confidencialidad, integridad y disponibilidad.

La norma permitirá seleccionar los objetivos de control y los controles para poder contrarrestar vulnerabilidades que puedan llegar a afectar este activo de información teniendo como base la evaluación del riesgo y su tratamiento.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La información es el activo más valioso dentro de toda organización, es por ello que es de vital importancia aplicar las medidas y procedimientos necesarios para garantizar su disponibilidad, confidencialidad e integridad. Actualmente existe un alto nivel de exposición de este activo, mismo que está relacionado con la utilización e implementación de nuevos recursos informáticos que sin bien es cierto contribuyen a mejorar la productividad y a lograr mejores resultados y objetivos también lo posicionan en el centro de posibles vulnerabilidades y amenazas.

La organización debe tener claro cuáles son los activos que desea proteger y que son necesarios para el normal funcionamiento del negocio, armando una estrategia apropiada que le permita continuar con sus operaciones en caso de que llegare a ocurrir alguna eventualidad, para ello requiere definir un plan de continuidad de negocio donde se identifiquen los posibles escenarios de amenazas que se puedan hacer presente debido al crecimiento de las redes y de la cantidad de usuarios que se interconectan a las mismas, sumando a lo anterior la mala práctica de utilizar tecnologías con poca madurez en el ámbito de la seguridad y que son lanzadas al mercado para ser consumidas por los usuarios que las requieren.

Cuando una amenaza se materializa luego de aprovechar una vulnerabilidad, las operaciones del negocio se ven expuestas a un riesgo. Este riesgo lleva consigo la posibilidad de impactar de forma negativa a los recursos definidos como primordiales por la organización trayendo como consecuencia la paralización de sus operaciones ya sea de forma temporal o permanente. Los riesgos pueden ser financieros, operacionales, ambientales y tecnológicos y por ello es importante definir controles que permitan mitigar o minimizar el impacto que una amenaza pueda llegar a tener sobre un determinado activo.

Este proyecto de titulación basa su análisis en la aplicación de la norma ISO 27001:2013, como un estándar con reconocimiento en el mercado tanto nacional como internacional que provee de los recursos necesarios para gestionar la seguridad de la información de una determinada organización que para nuestro caso de estudio está dirigido a una compañía de seguros.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

Las empresas de seguros por su naturaleza requieren de sus clientes información que sirve para verificar cada objeto asegurable y valorar el riesgo que representa. Esta valoración incluye la verificación del origen de dichos objetos es decir que provenga de situaciones lícitas y por ello la empresa aseguradora tiene la potestad de solicitar toda la información que requiera para de esta forma otorgar el alcance que un determinado seguro puede tener, tales como coberturas, cláusulas, beneficiarios, etc., dentro del documento llamado póliza.

La póliza es un documento donde se detalla de forma general y particular las condiciones convenidas entre el asegurado (cliente) y el ente asegurador (Empresa de Seguros), así como el/los bienes que se requieren asegurar y las coberturas que son asumidas por la entidad aseguradora.

Es por esta razón que a través de la póliza el cliente queda vinculado a la empresa de seguros, convirtiéndose esta última en el principal custodio y protector de la información que ha recibido.

1.2 DESCRIPCIÓN DEL PROBLEMA

El principal problema radica en la falta de estrategias para que la información que proviene del proceso de emisión de pólizas sea tratada como un activo importante y pueda cumplirse con los principios de la seguridad: la confidencialidad, disponibilidad e integridad. Al no existir controles, políticas y procedimientos que ayuden a detectar amenazas que puedan poner en riesgo dicho activo, puede traer como consecuencia que la información del cliente caiga en manos equivocadas, provocando pérdida de negocios y demandas legales.

Al existir un riesgo presente es preciso definir con precisión los controles necesarios que permitan establecer, implantar, operar, monitorear, mantener y mejorar la seguridad de la información.

Motivo por el cual a nivel general sus principales problemas radican en la falta de:

- Políticas de contratación de pólizas de seguros.
- Nivel de comunicación entre el asegurado, mediador y entidad aseguradora a la hora de contratar y modificar las pólizas de seguros.
- Capacitación al personal.
- Manuales de procedimientos.
- Contraseñas seguras y la no divulgación de las mismas.
- Transmisión de información por medios inseguros.
- Control en los errores de programación en las aplicaciones.
- Mecanismos de mitigación de riesgos

1.3 SOLUCIÓN PROPUESTA

Desarrollar un plan de riesgos de seguridad para el proceso de emisión de pólizas basado en la norma ISO 27001:2013, norma que define las acciones para lograr dicho objetivo. El uso de este esquema permitirá evaluar de manera adecuada los riesgos en referencia a los activos de información, de tal forma que se puedan establecer controles y realizar la valoración necesaria para contrarrestar las vulnerabilidades y amenazas y con ello mejorar la eficacia y eficiencia de la empresa aseguradora.

Al tener la póliza información tanto personal, como crediticia del cliente, se convierte en el principal activo de información y por lo tanto su grado de criticidad es alto por lo que debe cumplir con las características básicas de la seguridad de la información como son: la confidencialidad, integridad y disponibilidad.

La norma permitirá seleccionar los objetivos de control y los controles para poder contrarrestar vulnerabilidades que puedan llegar a afectar este activo de información, teniendo como base la evaluación del riesgo y su tratamiento.

Como se llevará a cabo esto:

- Identificando los activos de información del proceso de emisión de pólizas
- Realizando la valoración de los riesgos
- Analizando y diseñando el plan de riesgo (Tratamiento de riesgo)
- Implementado el plan de riesgo.

Para la realización de estos puntos se procederá en primer lugar con el levantamiento de la información sobre los riesgos, activos, programas, procesos y procedimientos actuales del negocio, para luego continuar con el diseño y

análisis en base a la información recogida de tal forma que se puedan implementar y desarrollar los pasos, culminando con el análisis de los resultados y la consecuente verificación de que cumpla con los objetivos establecidos.

1.4 OBJETIVO GENERAL

Desarrollar un plan de riesgos de seguridad para el proceso de emisión de pólizas para una Empresa de Seguros del Ecuador, siguiendo la norma ISO 27001:2013 con el propósito de mitigar los riesgos inmersos en dicho proceso.

1.5 OBJETIVOS ESPECÍFICOS

- Analizar la situación actual de la empresa a través del departamento de Operaciones.
- Realizar el levantamiento de información en referencia al proceso de emisión de pólizas.
- Identificar los activos de seguridad que están dentro del proceso de emisión de pólizas de la Empresa.
- Diseñar el Plan de tratamientos de riesgos del proceso de emisión de pólizas de la Empresa.
- Implementar los resultados del plan de tratamiento de riesgos y verificar que cumpla con los objetivos planteados.

1.6 ALCANCE

- Establecer una adecuada administración de riesgos.
- Establecer que los recursos de la empresa sean utilizados de forma adecuada.

- Obtener resultados medibles.
- Mejorar la confianza de las partes involucradas
- Mejorar los controles
- Mejorar la probabilidad de alcanzar objetivos

1.7 METODOLOGÍA

La gestión de la seguridad de la información no constituye solo un tema técnico puesto que se requiere del apoyo de la Gerencia así como también del acoplamiento de los procesos o actividades que desempeña la organización, motivo por el cual los controles y formas de mitigación de cualquier riesgo que pudiere ocurrir, debe estar acorde a las necesidades del negocio.

La norma ISO/IEC 27001 proporciona los controles así como también los delineamientos para la gestión de la seguridad de la información, cada uno de sus procesos y dominios, permite tener una guía de implementación basada en procedimientos explícitos y ordenados.

Los principales procesos que se enmarcan en esta norma se encuentran identificados con las etapas del ciclo PHVA (Planear, Hacer, Verificar, Actuar). Por lo que se seguirán los procesos que se encuentran inmersos en cada una de las etapas, más, cabe indicar que la tesis solo abarcará el planeamiento e implementación, con lo que tenemos entonces:

Planear:

- Se definirá alcance y límites
- Se definirá el enfoque para evaluar los riesgos
- Se identificarán los riesgos

- Se evaluarán alternativas para el plan de tratamiento de riesgos

Hacer:

- Se implementará un plan de tratamiento de riesgos
- Se definirán métricas para cada riesgo
- Se implementarán programas de aceptación y asimilación del riesgo
- Se implementarán métodos y controles para lidiar con la gestión de incidentes de seguridad

La metodología estará dividida en etapas concatenadas, cuestión que permitirá el avance paulatino y ordenado donde no se podrá continuar con la siguiente etapa sino se ha terminado con la anterior.

Bajo esta primicia la metodología que se aplicará estará basada en los siguientes puntos:

- Técnica de la observación mediante entrevistas programadas con los diferentes entes que intervienen en el proceso de emisión de pólizas, tales como: emisores, personal de sistemas y comerciales.
- Se aplicará la metodología ISO/IEC 27001 para realizar el análisis y evaluación de los riesgos, de tal forma que se logre la protección de los datos tomando en consideración los principios fundamentales de confidencialidad, integridad y disponibilidad de la información.
- Se usará en estándar MAGERIT versión 3.0 para valorar los riesgos, identificando posibles amenazas y a su vez clasificando los riesgos para de esta forma poder definir un sistema de control de seguridad para el proceso de emisión de pólizas.

- Se aplicará la norma ISO/IEC 27002 para verificar la existencia de controles mediante listas de chequeo.
- Mediante el uso de preguntas o cuestionarios se procederá a validar la posible existencia de amenazas y vulnerabilidades que pueden llegar a interferir con el normal desenvolvimiento del proceso de emisión de pólizas.
- Se realizará la valoración de los riesgos en base a dos escalas: Escala de probabilidad de ocurrencia y escala de valoración de impacto.
- Se definirá el tratamiento para los riesgos de acuerdo a los controles proporcionados por la norma ISO/IEC 27002 para luego incluirlos como política y procedimientos organizacionales.

Es importante indicar que algunos de los problemas de seguridad de las diferentes organizaciones, ocurren por la falta de conocimiento de las políticas y normas implementadas para gestionar la seguridad de la información, por ello dichas políticas y normas debe formar parte de la cultura organizacional para de esta forma poder minimizar los riesgos o amenazas que pudieren afectar al negocio y en este caso al proceso de emisión de pólizas.

CAPÍTULO 2

MARCO TEÓRICO

2.1 SEGURIDAD INFORMÁTICA

La seguridad informática permite cuidar los recursos de los sistemas de información de una determinada organización, ayudando a garantizar la confidencialidad, integridad y disponibilidad por medio de procedimientos y herramientas definidas para de esta forma evitar daños y minimizar los riesgos[7].

Los principios de la seguridad informática están determinados por tres aspectos fundamentales como son:

a) **Integridad:** Se refiere a la consistencia y garantía de los datos.
b) **Confidencialidad:** Se refiere a la privacidad de los datos.
c) **Disponibilidad:** Se refiere a la accesibilidad de los datos cuando sean requeridos.

Hoy en día con el crecimiento del uso del internet y la necesidad de conexión que tienen los empleados de una organización por acceder a los diferentes sistemas

de información, el control de los accesos y su debido aseguramiento se convierte en un tema fundamental que debe ser considerado y puesto en marcha, ya que una intrusión no autorizada puede llegar a causar graves problemas.

Cuando ocurren este tipo de eventos, la pérdida de datos es la principal consecuencia, así como el robo de información, por lo que para tomar las medidas correctas es preciso que se tenga el pleno conocimiento de las amenazas, vulnerabilidades y las intenciones dañinas que puedan llegar a presentarse, con la finalidad de poder contrarrestarlas, es decir se debe conocer el peligro, clasificarlo y protegerlo implementando los mecanismos necesarios para ello[3].

La amenaza es un riesgo que se evidencia por una acción que por lo general es dañina y la vulnerabilidad indica la falta de control ante esta amenaza, se debe entonces tratar de prever todo aquello que se haga susceptible a dicho riesgo.

Es válido indicar que no existe la seguridad absoluta, puesto que al no tener la certeza de cuándo ocurrirá un determinado evento, el riesgo siempre estará presente independientemente de las medidas que tomemos. Por ello es de suma importancia definir claramente los elementos que deben ser protegidos, con la finalidad de minimizar el impacto ante una amenaza latente, tales como: software, hardware y los datos, siendo este último el más susceptible y más difícil de recuperar, por lo que debe ser tratado con mayor atención.

Es preciso entonces potenciar las políticas de seguridad de tal forma que se pueda garantizar la reducción de las vulnerabilidades y con ello reducir los niveles de exposición de las organizaciones.

2.2 SEGURIDAD DE LA INFORMACIÓN

Siendo la información el activo más valioso de toda organización, es necesario establecer medidas que busquen protegerla de amenazas que pueden llegar a afectar la continuidad de la empresa [7].

Los sistemas de información contienen la información que reside en equipos informáticos, almacenamientos tanto internos como externos y redes de datos, por lo cual está expuesta y es susceptible a amenazas tanto internas como externas. Es por esta razón que se deben establecer medidas para protegerla de tal forma que se pueda garantizar la confidencialidad, integridad y disponibilidad de la misma.

El sistema de gestión de seguridad de la información (SGSI), es una herramienta valedera a la hora de implementar un procedimiento que permita cuidar, revisar y supervisar la seguridad de la información. Para ello utiliza el ciclo PDCA que permite establecer la mejora continua con la cual es posible obtener un nivel de seguridad satisfactorio [3].

Es preciso que la empresa defina la seguridad de la información como prioridad, instalando mecanismos que logren mitigar la mayor parte de los riesgos a la que se encuentra expuesta la información del negocio. El éxito de estas medidas se basa en definir claramente los objetivos que se desean implantar teniendo en consideración tanto las leyes del lugar donde se desarrolla la organización como el día a día de sus operaciones.

Los controles o medidas que se implementen deben ser revisados periódicamente, de tal forma que se puedan detectar errores en los controles que se destinaron para proteger la información y deben estar orientados tanto a los

sistemas que contienen los datos como a los equipos que se utilizan para acceder a ellos.

Así mismo, debe considerarse la difusión de dichas medidas para asegurar que sean cumplidas y que están acorde con la realidad del negocio. Se entiende por ello que la seguridad de la información es sumamente importante puesto que constituye un compromiso de aseguramiento y concienciación de la información por parte de la organización, estableciendo objetivos y direccionando recursos tanto económicos como humanos para su consecución [13].

2.3 ADMINISTRACIÓN DE LA SEGURIDAD

La administración de la seguridad busca monitorear los objetivos definidos para la seguridad de la información. Para ello es importante promover la seguridad de la información haciéndola formar parte de los delineamientos de la organización.

Actualmente existen múltiples riesgos para los sistemas de información, por lo que es necesario contrarrestarlos implementando controles basados en normas y estándares internacionales y alineándolos a las leyes existentes.

Dichos riesgos ponen sobre el tapete las diferentes vulnerabilidades a las que se exponen los negocios hoy en día. Estas vulnerabilidades pueden ser internas o externas y pueden llegar a repercutir enormemente en las operaciones y continuidad de la organización. Por ello se deben establecer políticas, procedimientos y controles que sirvan de base para evitar o disminuir cualquier riesgo que llegare a presentarse y administrarlos de manera eficiente para verificar que el objetivo para los cuales fueron creados se cumpla [14].

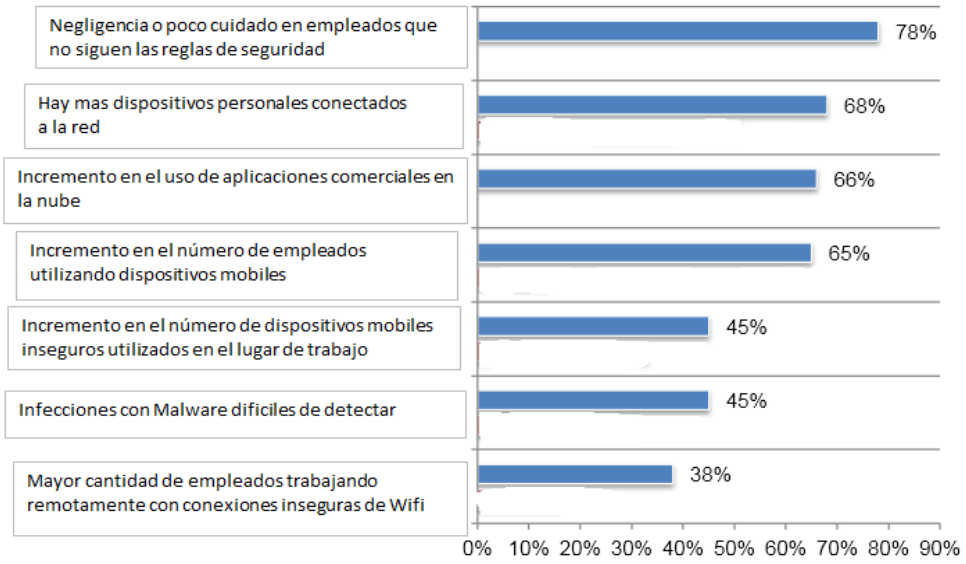


FIGURA 2.1 Factores que contribuyen a riesgos de seguridad.
Autor: PONEMON INSTITUTE REPORT (Año 2.014)

Para que la administración de la seguridad sea la adecuada, es importante haber identificado los riesgos asociados a un determinado proceso, así como su correspondiente definición y las medidas para mitigarlos. El mantenimiento que se le dé a estas medidas mediante revisiones periódicas, permitirá corregir errores y evaluar los resultados de implementación para estos procedimientos [9].

Aunque se han obtenido grandes avances en cuanto a la seguridad y la protección de datos, bien sea por mejora en equipos, redes, accesos, aplicativos, etc., no existe todavía un método que permita minimizar pérdidas y reducir costos de recuperación, puesto que mientras vaya en aumento el uso del internet para acceder a los diferentes sistemas de información siempre existirá un riesgo y es por esa razón que la administración de la seguridad debe aprovechar la integración de los componentes de seguridad a su plan de acción.

La norma ISO/IEC 17799 establece 10 dominios de control que cubre casi por completo la Gestión de Seguridad del a información, alguna de ellas: Continuidad del negocio, Políticas de Seguridad, Control de accesos, etc[1].

Debiendo evaluarse los que se acoplan de mejor manera a la organización para poder ponerlos en práctica.

2.4 ANÁLISIS DE RIESGOS

La gestión de riesgos es una parte fundamental del negocio ya que permite conocer las vulnerabilidades a las que se hayan expuestos los activos de información. La gestión de riesgos forma parte del SGSI (Sistema de Gestión de Seguridad de la Información) y existen varios procedimientos o metodologías que se pueden aplicar para llevar a cabo esta actividad[3][13].

El análisis de riesgos debe proporcionar una evaluación económica del impacto de un determinado evento, cuestión que se logra identificando los recursos con que se cuenta y las amenazas a las que están expuestos.

Por ello es importante clasificar todos los recursos de la organización de tal forma que se pueda documentar e identificar todas las amenazas posibles, evaluar el nivel de criticidad del riesgo y los puntos de acción necesarios para hacerles frente, estableciendo los controles que lleguen a mitigar dichos eventos. Cuando una amenaza se vuelve viable se abre la puerta a una vulnerabilidad poniendo en exposición o riesgo un determinado activo, cuestión que ocasiona pérdidas de información o intrusiones no deseadas que pueden llegar a tener un impacto negativo en la organización.

Las fases para el análisis de riesgo incluyen:

- Identificar los activos
- Evaluar las amenazas
- Realizar el tratamiento del riesgos

Dentro de la identificación de los activos se debe reconocer todos los elementos que componen el sistema de información y que pueden llegar a sufrir una amenaza. La evaluación de las amenazas consiste en determinar los eventos que pueden llegar a afectar la integridad de los procesos. Estos eventos pueden ser: naturales, intencionales o accidentales. Una vez que hayamos identificado las amenazas es importante verificar el riesgo que será afectado por dicha amenaza [14][20][21].

El tratamiento del riesgo corresponde a encontrar el equilibrio entre el nivel de seguridad y su costo, incluye además la toma de decisiones para aceptar, transferir y reducir el riesgo.

Las ventajas de realizar el análisis de riesgos son:

- Verificar las áreas que son susceptibles a una amenaza.
- Identificar nuevos riesgos ante posibles cambios de arquitectura.
- Establecer mecanismos y determinar el gasto que este infiere.
- Aumentar la confianza entre los actores del negocio.

El análisis de riesgo puede ser llevado a cabo mediante diferentes análisis, así tenemos:

Análisis Cualitativo

Este método se basa en el juicio, experiencia e intuición, es factible utilizar este método cuando el riesgo es bajo y no se justifica un análisis de riesgo completo o

porque los datos numéricos son inadecuados. Entre los métodos cualitativos están:

- Lluvia de ideas
- Cuestionario y entrevistas estructuradas
- Evaluación para grupos multidisciplinarios
- Juicio de especialistas y expertos

Análisis Semi-Cuantitativo

Se realizan descripciones más detalladas de la probabilidad y consecuencia o clasificación de palabras como alto, medio o bajo, dicha clasificación se enmarca en una escala de cálculo de nivel de riesgo.

Análisis Cuantitativo

Permite calcular el nivel del riesgo, incluyendo procedimientos de: Análisis de probabilidad, Análisis de consecuencias y Simulación computacional.

Hoy en día existen en el mercado diferentes metodologías, normas o estándares que ayudan a realizar el análisis de riesgo, tales como: OCTAVE, MAGERIT, ISO 27005, etc.

OCTAVE (OPERATIONALLY CRITICAL THREAT ASSET AND VULNERABILITY EVALUATION)

OCTAVE es una metodología de análisis de riesgos que le permite a la organización: Dirigir y gestionar evaluaciones de riesgos, tomar decisiones, proteger los activos de información y comunicar de manera efectiva las políticas de seguridad.

La definición del riesgo y sus amenazas se realiza mediante la evaluación de activos críticos, basada en prácticas normales del negocio de tal forma que se puedan incluir estrategias de protección y mitigación. Entre los beneficios del uso de OCTAVE tenemos:

- Se pueden identificar los riesgos que pueden afectar al negocio.
- Permite evaluar dichos riesgos.
- Permite crear una estrategia que permite reducir los riesgos.
- Dar cumplimiento a regulaciones relacionadas con la seguridad de la información.

MAGERIT

MAGERIT es una metodología que se alinea con los estándares ISO 27005 e ISO 31000, permite identificar las amenazas y vulnerabilidades así como las medidas preventivas y correctivas que se ajusten al negocio. Esta metodología fue creada para ser usada en el área pública de España, más hoy por hoy su uso se ha extendido ya que permite analizar los riesgos e implementar medidas para mitigar las amenazas que de ellos se derivan[4][5].

MAGERIT implementa el proceso de gestión de riesgos dentro de un marco que permite la toma de decisiones a partir de los riesgos derivados por el uso de tecnologías de información.

FIGURA 1.2 Marco de trabajo para la gestión de riesgos
Fuente: Tomado del Libro 1 de Magerit versión 3

MAGERIT consta de tres libros:

- Método
- Catálogo de elementos
- Guía de técnicas

Método

Está compuesto por ocho capítulos mismos que describen como formalizar las actividades de análisis de riesgos, de gestión de riesgos, de planes de seguridad, permitiendo establecer criterios de tratamiento de riesgos y el análisis necesario para gestionar la seguridad del producto final.

Catálogo de elementos

Ofrece elementos estándar para realizar el análisis de riesgo, tanto a nivel de terminología como de criterios.

Guía de técnicas

Ofrece orientación adicional sobre técnicas que se emplean de manera regular en el análisis y gestión de riesgos, tales como: Análisis mediante tablas, algorítmico, técnicas gráficas y árboles de ataque.

2.5 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad son un conjunto de reglas que deben ser divulgadas, entendidas y seguidas por cada miembro de la organización. A nivel de seguridad de la información, indica una serie de procedimientos que deben ser llevados a cabo con la finalidad de mitigar el riesgo que pude ocasionar una eventual amenaza y de esa forma evitar pérdidas o accesos no autorizados a la organización[21].

La política de seguridad tiene como principal objetivo entonces, la implementación de leyes, normas y prácticas que garanticen la confidencialidad, disponibilidad e integridad de la información y que las mismas puedan ser entendidas por todos los miembros de la organización.

Dichas políticas pueden ser detalladas o generales, esto depende del grado de madurez del negocio y de su capacidad económica para aceptar el riesgo, puesto que el costo de la seguridad resulta considerablemente alto y no se es posible tener un esquema cien por ciento seguro.

Es por ello que estas políticas surgen como una herramienta de la organización para concientizar a cada uno de sus miembros sobre el tratamiento de la información y establecer un compromiso que permita reconocer fallas o procesos

ineficaces para ir actualizando estas políticas a la par de los requerimientos del negocio.

Sea cual fuere la política a implementar, esta debe contemplar los elementos claves de la seguridad como son: Integridad, Confiabilidad y Disponibilidad, así como también los tipos de amenazas que hacen vulnerables nuestros procesos:

- Amenazas del Sistema
- Amenazas de la Red
- Amenazas de Personas
- Desastre del Entorno

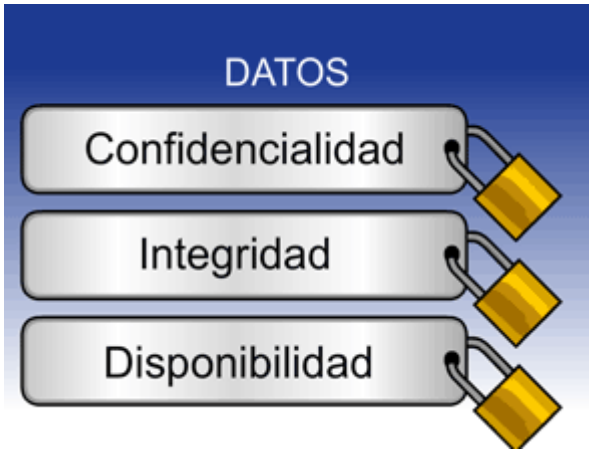


FIGURA 2.3 Confidencialidad, Integridad y Disponibilidad de los Datos

Para que una política de seguridad rinda los frutos esperados, es necesario que sea reconocida por las personas relevantes dentro de la organización. Es preciso que se entienda que la definición de esquemas o normas de seguridad ayudarán a proteger a la organización de los riesgos que se derivan a partir del uso de tecnologías. Es por esto que dichos esquemas deben ser entendidos de forma natural y sin el uso excesivo de tecnicismos, que lo único que ocasionan es

desinformación y la resistencia hacia estos nuevos modelos, dejando expuestos los activos a un sinnúmero de amenazas.

2.6 DESARROLLO DEL MODELO DE SEGURIDAD SEGÚN EL ESTÁNDAR INTERNACIONAL ISO 27001:2013

Para que una política de seguridad rinda los frutos esperados, es necesario que sea reconocida por las personas relevantes dentro de la organización. Es preciso que se entienda que la definición de esquemas o normas de seguridad ayudarán a proteger a la organización de los riesgos que se derivan a partir del uso de tecnologías. Es por esto que dichos esquemas deben ser entendidos de forma natural y sin el uso excesivo de tecnicismos, que lo único que ocasionan es desinformación y la resistencia hacia estos nuevos modelos, dejando expuestos los activos a un sinnúmero de amenazas [1].

De acuerdo a la norma ISO 27001 la seguridad de la información consiste en conservar la integridad, disponibilidad y confidencialidad de la información que se genera dentro de un negocio. Esta norma por lo tanto, especifica los procedimientos, métodos o pasos a seguir para para implementar, monitorear, mantener y revisar un ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) o SGSI (Sistema de gestión de seguridad de la información).

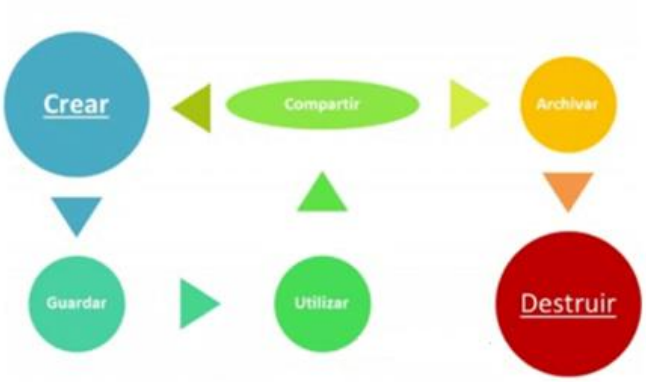


FIGURA 2.2 Fuente: ISO 27000.es

El sistema de gestión de seguridad de la información conocida como SGSI o en sus siglas en inglés ISMS INFORMATION SECURITY MANAGEMENT SYSTEM, constituye el referente de la norma ISO 27001. Su principal objetivo es lograr que los riesgos derivados de la seguridad de información, sean asumidos, conocidos, gestionados y minimizados de forma ordenada y documentada y que puedan ser adaptables a los cambios que pueda tener la organización.

FIGURA 2.3 Fuente: ISO 27000.es

Es importante considerar que la información es un activo que posee un valor importante y no importa cómo se guarde o transmita, esta debe ser protegida mediante un procedimiento sistemático y documentado que debe ser conocido por toda la organización y es a este proceso que se lo conoce como SGSI.

ISO 27001 indica que un SGSI debe tener los siguientes documentos:

- **Alcance del SGSI:** Incluye la identificación de las áreas y procesos donde se aplicará el SGSI así como las partes donde no se lo considerará.
- **Política y objetivos de seguridad:** Muestra un enfoque de la organización en relación con el SGSI.
- **Procedimientos y mecanismos de control que soportan al SGSI**: Son los procedimientos y mecanismos de control en los que se basa el SGSI para su desarrollo.
- **Enfoque de evaluación de riesgos:** Especifica los procedimientos o métodos que tienen que ver con el manejo de las amenazas, vulnerabilidades y bajo cuales criterios serán solventados.
- **Informe de evaluación de riesgos:** Se muestra el resultado de la aplicación de la metodología sobre los activos que pertenecen al negocio.
- **Plan de tratamiento de riesgos:** Son las acciones que toma la gerencia en relación a la forma de gestionar los riesgos involucrados con la información.
- **Procedimientos documentados:** Corresponde al seguimiento que se realiza para asegurar la eficacia de la metodología implementada para contrarrestar los diferentes riesgos que pueden ocurrir.
- **Registros:** Representan las evidencias soportadas como base para el funcionamiento efectivo del SGSI.

- **Declaración de aplicabilidad:** Se basa de forma específica en los procesos y tratamiento de riesgos y como serán mitigados, controlados y evaluados dentro del SGSI.

En todo caso el ISO 27001 provee lo necesario para la creación del ISMS, incluyendo la lista de controles para los riesgos y la forma de mitigar los mismos.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

3.1 ANTECEDENTES DE LA EMPRESA

La empresa de seguros es una multinacional que opera en el Ecuador desde hace setenta años con sucursales en Quito y Cuenca. Al ser una empresa de seguros, su principal actividad es la venta de seguros, para bienes muebles, inmuebles y personas.

El comienzo de la actividad comercial en dicha empresa, inicia con la recopilación de los datos necesarios para el armado de la póliza. La póliza por lo tanto pasa a ser el principal instrumento que contiene toda la información necesaria para satisfacer tanto la auditoría interna requerida por las regulaciones existentes en el mercado, así como también los requerimientos de las entidades reguladoras que pertenecen al estado, como son: Superintendencia de Compañías, Unidad de Análisis Financiero, Prevención de Lavado de Activos y Servicio de Rentas Internas.

La junta de accionistas define en modo general como se llevará a cabo el proceso de emisión de pólizas, más es el área de Operaciones, representada por el Gerente de Operaciones quien establece los controles que servirán para dar fiel cumplimiento a las normas establecidas por las entidades anteriormente mencionadas.

El proceso de emisión de pólizas es realizado de forma íntegra por el Departamento de Operaciones, mismo que está conformado de la siguiente manera:

- Gerente de Operaciones
- Jefe de Emisiones
- Auxiliares de Emisiones

El Gerente de Operaciones es el encargado de controlar todo el flujo de la emisión de pólizas, desde que el cliente se acerca a la compañía a solicitar el seguro hasta su contabilización y reaseguramiento, además de la administración post-emisión de los siniestros en caso de que ocurran. Es también el encargado de hacer la evaluación inicial del riesgo que representa el bien asegurado, clasificándolo de la siguiente forma:

- **Riesgo Moral**

Al ser la póliza o contrato de seguro un contrato de buena fe, la importancia de evitar que los mismos sean utilizados en actividades incorrectas tales como: Lavado de Activos o enriquecimiento ilícito es algo por lo que debe velar la compañía ya que está estipulado en las leyes ecuatorianas, motivo por el cual se convierte en un deber de la compañía el contribuir con la sociedad para que todos sus actos se enmarquen en actividades lícitas y de honestidad.

- **Riesgo físico**

El objeto o cosa asegurada que interviene en el proceso de emisión de pólizas debe ser verificado para constatar que sea tangible y que se encuentre en buenas condiciones, por ello toda la información entregada por el cliente debe ser inspeccionada y evaluada para que el contrato pueda ser suscrito.

- **Riesgo Operativo**

Está vinculado directamente con la actividad del negocio y para nuestro caso con el proceso de la emisión de una póliza, de lo que se deriva:

a) Errores de tarificación

b) Errores en el diseño del producto que se oferta

c) Errores en la selección y aprobación del objeto asegurable.

d) Errores en el establecimiento de políticas inadecuadas de venta

e) Errores de digitación de datos

f) Errores de procedimiento de entrega de documentos del asegurado por parte del bróker de seguros

g) Errores por desconocimiento de ciertas tareas realizadas por los asistentes de emisión

h) Errores por falta de comunicación entre técnico y emisor.

3.2 IDENTIFICACIÓN DEL PROCESO

ISO 27001 es considerada como la norma internacional con más prestigio a nivel mundial en lo que se refiere a la seguridad de la información y es por lo pronto la norma que ofrece una solución de mejora continua que permite la evaluación de los riesgos y el establecimiento de controles para cada uno de ellos.

Esta norma se enfoca en los procesos para todo el ciclo del SGSI, dichos procesos están compuestos generalmente por un conjunto de actividades que consumen recursos, sean estos: humanos, materiales o económicos.

Los procesos están compuestos por actividades, mismas que se llevan a cabo a partir de procedimientos, delineamientos o instrucciones que indican el responsable y el tiempo en que deben ser ejecutadas, de tal forma que las salidas que resulten de dicha actividad sean utilizadas de forma idónea por otros procesos, que para este caso son: Reaseguros, Cobranzas, Siniestros y Contabilidad.

Para poder medir, mitigar, administrar y mejorar los procesos es preciso conocerlos y entenderlos, de esta forma se los puede controlar y lograr que tengan resultados previsibles y satisfactorios. Para conseguir este objetivo es necesario asignarle indicadores de medición, objetivos y políticas.

La emisión de la póliza para la compañía de seguros representa un proceso estratégico y operativo que está compuesto por otros subprocesos que a su vez se componen de actividades que deben ser llevadas a cabo una vez que el cliente o bróker han indicado su deseo de adquirir el seguro. Estas son:

- Inspección del bien o persona asegurable.
- Selección de tasas, coberturas, cláusulas.
- Conocimiento del cliente
- Selección del reaseguro
- Cotización del bien o persona asegurable.
- Facturación de la póliza.

El proceso de emisión de pólizas se muestra en el gráfico presentado a continuación.

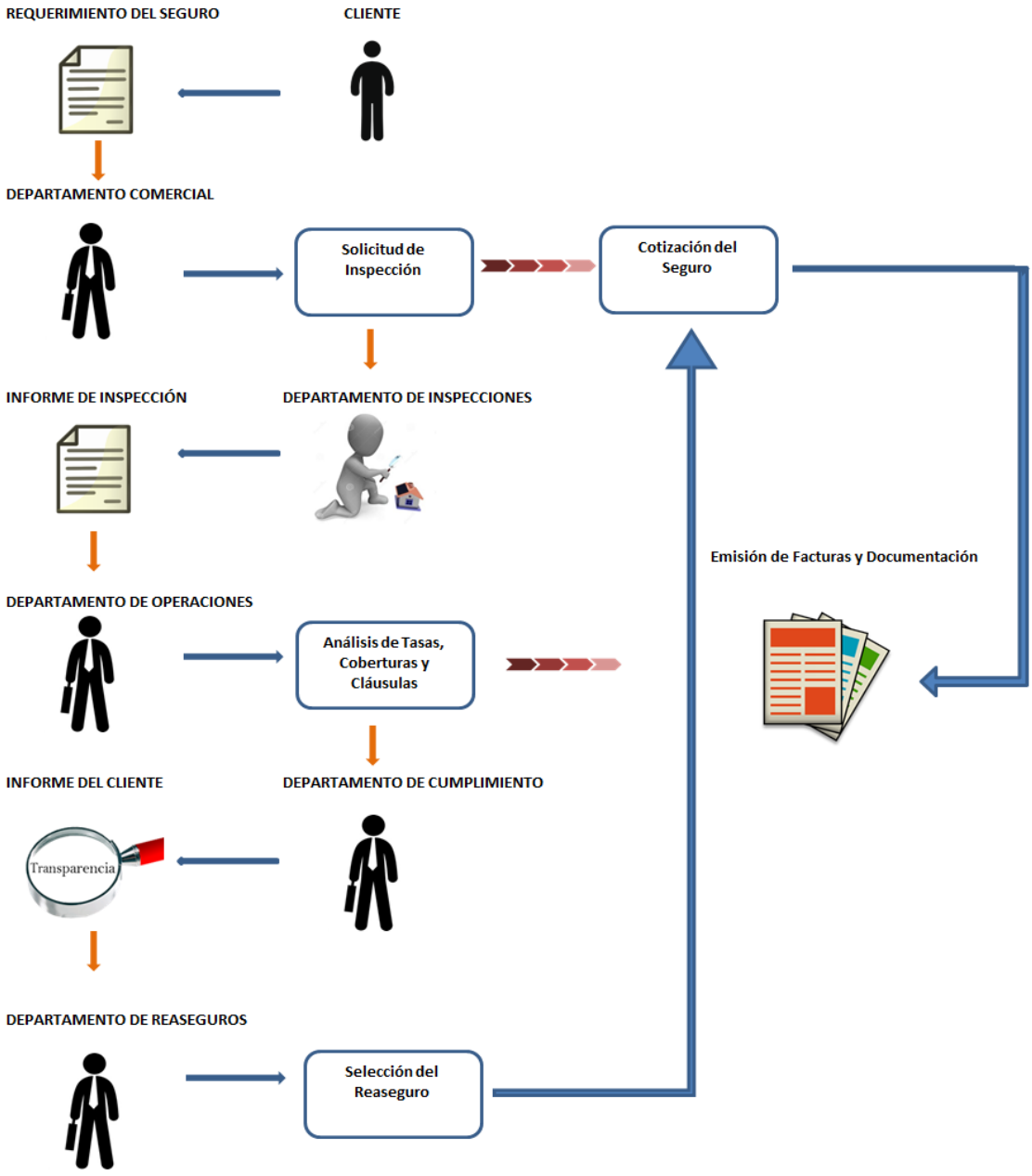


FIGURA 3.1 Proceso de Emisión de Pólizas Referencia: Autor

Como se indicó anteriormente el proceso de emisión de pólizas se compone por varios subprocesos que se activan en el momento que el cliente realiza la petición de un seguro. Dicha petición la realiza en primera instancia con el Departamento Comercial quien se encarga de dar viabilidad a la solicitud que comienza a activar los subsiguientes subprocesos.

El subproceso de Solicitud de Inspección es realizado por un inspector de riesgos y no es otra cosa que la recolección de información en referencia al bien asegurable. Es por lo tanto un subproceso netamente operativo ya que su finalidad es recabar la mayor cantidad de información que sirva para evaluar e identificar al riesgo y con esto verificar las medidas de protección o exposición que tiene para que la empresa de seguros posea las herramientas necesarias y esté en capacidad de aceptarlo o rechazarlo.

El subproceso de Análisis de Tasas, Coberturas y Cláusulas está ligado de forma técnica con la operación del negocio, puesto que se basa en las políticas de cobro establecidas por la compañía de seguros y reguladas por la Superintendencia de Compañía[1]. De la misma forma las condiciones particulares contendrán las coberturas y cláusulas que la compañía oferta y que además han sido debidamente aprobadas por la entidad del estado anteriormente nombrada y que está dada en base a su línea de negocio.

El subproceso de cumplimiento o conocimiento del cliente, es operativo y es realizado por la Unidad de cumplimiento, su objetivo es prevenir actividades que tiendan a financiar el terrorismo, lavado de activos u otros delitos que puedan involucrar a la empresa de seguros mediante la contratación de la póliza. Para

[1] ***La Superintendencia de Compañías es el organismo técnico, con autonomía administrativa y económica, que vigila y controla la organización, actividades, funcionamiento, disolución y liquidación de las compañías y otras entidades en las circunstancias y condiciones establecidas por la Ley.***

ello la empresa a través de la unidad de cumplimiento tiene implementadas diferentes políticas tales como: Política de conozca a su cliente, política de conozca a su empleado, política de conozca a su mercado.

Dichas políticas se basan específicamente en la confirmación y actualización de los datos del cliente, empleado y mercado, así como la verificación en las listas negras, las catalogadas PEPS (Personas políticamente expuestas), las listas del CONSEP, OFAC, entre otros.

El subproceso de selección de reaseguro es operativo y se conoce como el seguro para el seguro. Lo que busca es verificar la exposición del bien asegurable y determinar si el mismo puede ser cubierto en su totalidad por la compañía de seguros o debe utilizarse un contrato alterno de tal forma que se pueda trasladar el riesgo parcial o totalmente. Establece porcentajes y límites en base al capital asegurado entregado por el cliente.

El subproceso de cotización del seguro está ligado con la negociación que se llevará a cabo con el cliente, puesto que en él se plasma el costo del seguro, así como lo que la empresa aseguradora está dispuesta a cubrir para solventar la necesidad del cliente.

Es realizado por el Departamento Comercial quien se encarga de comunicarle al cliente el nivel de cobertura que goza y lo términos generales y particulares del contrato de seguros.

Finalmente luego de la aceptación del cliente de lo expuesto por el Departamento Comercial, los papeles son devueltos al Departamento de Operaciones quienes realizan la emisión de la póliza y su posterior facturación.

Otros procesos se activan luego de este último paso, tales como: contabilidad, caja, cobranzas, auditoría interna, talento humano y comité de riesgos, pero estos ya no forman parte de este estudio ya que este se basa únicamente en el proceso de emisión de pólizas.

3.3 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

De acuerdo a lo indicado por el libro 1 de Magerit [2] los activos son "Elementos que componen un sistema de información y que pueden ser atacados de forma accidental o malintencionadamente ocasionando riesgos para el negocio y sus diferentes operaciones. Estos activos pueden ser: Información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, parte administrativa y personas". Los activos de información son de vital importancia para el normal desenvolvimiento del negocio, motivo por el cual se debe identificar los activos de información para lograr determinar su grado de exposición y criticidad y en base a esto establecer las medidas que deben ser implementadas para contrarrestar cualquier amenaza en la que pudieran llegar a estar involucrados y evitar que con ello se detenga la operación del negocio.

A continuación se enlistan los activos de información involucrados en el proceso de emisión de pólizas:

Tabla 1 Identificación de Activos de Información

No.	Activo	Tipo de activo
1	Servidores	Hardware
2	Computadores/Laptops	Hardware

[2] ***2012_Magerit_v3_libro1_método_es_NIPO_630-12-171-8***

3	Impresoras	Hardware
4	Tablet/Cámaras fotográficas	Hardware
5	Socios, Auditores	Persona
6	Personal Administrativo	Persona
7	Sistema Integrado de Seguros	Software/ Información
8	Software de Facturación	Software/ Información
9	Software de Escaneo de Documentos	Software/Información
10	Sitio Web	Servicio
11	Servicio de correo electrónico	Servicio
12	Sistema de comunicación telefónica IP	Comunicaciones
13	Red de área local e inalámbrica	Comunicaciones
14	Informes llenados durante proceso	Datos/Soportes de información
15	Papeles de Trabajo/Documentos físicos	Datos/Soportes de información

3.4 TASACIÓN DE ACTIVOS

La tasación de activos permite conocer el valor que poseen los activos de una determinada organización, permitiendo conocer el nivel de protección requerido en base al impacto que tendría para el negocio al no cumplir con las normas estándares de confidencialidad, integridad y disponibilidad.

Bajo este razonamiento, si el impacto sobre el negocio es alto, entonces, el valor del activo deberá también ser alto.

El valor del activo se calcula en base a la afectación de la Integridad, Disponibilidad y Confidencialidad, para cuyo efecto se utiliza la siguiente fórmula:

(3.1)

$$A = \frac{i + d + c}{3}$$

Cuyos valores son:

A = Activo

i = Integridad

d = Disponibilidad

c = Confidencialidad

Para realizar la valoración de los activos en referencia al proceso de emisión de pólizas, se utilizará la Escala de Likert:

Tabla 2 Escala de Likert

1	2	3	4	5
Muy Bajo	Bajo	Medio	Alto	Muy alto

Tabla 3 Tasación de Activos Fuente: Autor

SUBPROCESOS	ACTIVOS	TIPO DE ACTIVOS	C	I	D	P
Requerimiento del Seguro	Papeles de Trabajo/Datos físicos – Solicitud de Seguro	Datos/Soporte de Información	3	5	5	4.33
	Sitio WEB	Servicio	3	3	4	3.33
	Red de Área Local e inalámbrica	Comunicación	4	4	4	4
	Sistema de Comunicación Telefónica IP	Comunicación	4	5	4	4.33
	Computadoras/Laptops	Hardware	5	5	3	4.33
	Servicio de Correo Electrónico	Servicio	5	5	4	4.66
	Personal Administrativo – Comerciales	Personas	5	5	3	4.33
Solicitud de Inspección	Tablet/Cámaras Fotográficas	Hardware	5	5	5	5
	Red de Área Local e	Comunicación	4	4	4	4

	inalámbrica					
	Personal Administrativo – Inspectores	Personas	5	5	3	4.33
	Computadoras/Laptops	Hardware	5	5	3	4.33
	Servicio de correo electrónico	Servicio	5	5	4	4.66
	Informe de Inspección	Datos/Soporte de Información	3	5	5	4.33
Análisis de Tasas, Coberturas y Cláusulas	Socios/Auditores	Personas	4	5	5	4.66
	Personal Administrativo –Gerencia de Operaciones	Personas	5	5	3	4.33
	Computadores/Laptops	Hardware	5	5	3	4.33
	Servicio de Correo Electrónico	Servicio	5	5	4	4.66
	Informe de Análisis de Tasa, Coberturas y Cláusulas	Datos/Soporte de Información	3	5	5	4.33
Colocación del Reaseguro	Personal Administrativo – Reaseguros	Personas	5	5	3	4.33
	Computadoras /Laptops	Hardware	5	5	3	4.33
	Servicio de Correo Electrónico	Servicio	5	5	4	4.66
	Informe de Reaseguro asignado	Datos/Soporte de Información	3	5	5	4.33
Cotización del Seguro	Servidores	Hardware	5	5	5	5
	Computadoras/Laptops	Hardware	5	5	3	4.33
	Impresoras	Hardware	5	5	5	5
	Sistema Integrado de Seguros	Software	4	4	4	4
	Personal Administrativo - Comerciales	Personas	5	5	3	4.33
	Servicio de Correo electrónico	Servicio	5	5	4	4.66
Emisión de Facturas y Documentación	Software de Facturación	Software	3	5	5	4.33
	Sistema Integrado de Seguros	Software	5	5	5	5
	Impresoras	Hardware	5	5	5	5
	Servicio de correo electrónico	Servicio	5	5	4	4.66
	Personal Administrativo – Operaciones	Personas	5	5	3	4.33
	Software de Escaneo de documentos	Software	4	4	4	4

3.5 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

De acuerdo a lo expuesto en el libro de Magerit [3] las amenazas son “cosas que ocurren”. Por lo que debemos tener presente el daño que puede sufrir cualquiera de nuestros activos si no existen los controles necesarios para mitigarlos o minimizarlos.

Siendo entonces las amenazas la causa de que una vulnerabilidad pueda llegar a afectar a nuestros activos y por ende al negocio, es preciso tenerlas identificadas para validar procedimientos, políticas o procesos que nos permitan mitigarlas. Entre las amenazas más comunes se encuentran:

1) De Origen Natural: Terremotos, inundaciones, maremotos, incendios forestales.
2) Del Entorno: Contaminación, fallos electrónicos, fuego, explosión
3) De Defectos: Problemas técnicos de equipos y aplicaciones.
4) Accidentales: De origen humano, errores u omisiones.
5) Deliberadas: De origen humano, tales como: Hacking, pérdida de datos.

Las amenazas no siempre afectan al activo en toda su dimensión y es por esta razón que debemos determinar qué tan perjudicado resultaría el activo y cuál es la probabilidad de ocurrencia del incidente. Para ello es necesario valorar dos puntos:

a) **Degradación:** El nivel de perjuicio del valor del activo.
b) **Probabilidad:** Posibilidad o imposibilidad que la amenaza se haga real.

[3] MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 – Método. Página 27.

Los activos de información por lo tanto están expuestos a múltiples amenazas, mismas que generan vulnerabilidades y Riesgos, tal como se muestra en el gráfico:

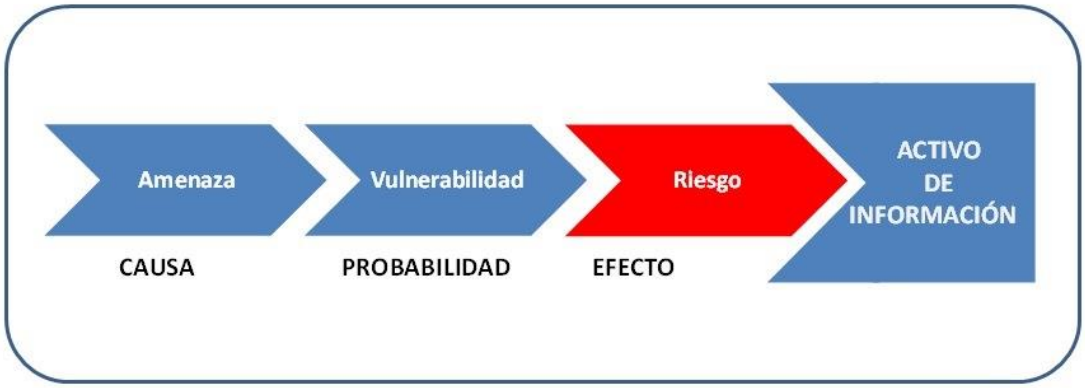


FIGURA 3.2 Elementos de análisis del riesgo. Fuente: Diseño de un Sistema de Seguridad de Información - Alberto G. Alexander

A continuación se detallan los activos con sus amenazas y vulnerabilidades:

Tabla 4 Identificación de Amenazas y Vulnerabilidades. Fuente: Autor

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada
Servidores	5	Accesos no autorizados	Puertas traseras activas, no detectadas
		Ataques por denegación de servicio	Tecnología insuficiente u obsoleta
		Robo de información relevante del negocio	Escasa administración y monitoreo de puertos abiertos
		Configuraciones susceptibles de copia.	Regular administración de sistemas.
		Fenómenos naturales	Edificación no apropiada y poco segura.
		Amenaza Física	Mala coordinación de mantenimientos de equipos
		Robo de contraseñas y permisos de archivos	Deficiente configuración de servicios no utilizados
		Pérdida de información relevante del negocio	Respaldos incompletos

		Acceso a privilegios de base de datos.	Parches inapropiados en equipos.
		Amenaza lógica	No disponibilidad por falta de redundancia
		Intrusiones a la red	Ausencia de políticas de contraseñas
		Caída del sistema por agotamiento de recursos	Cálculo inapropiado de consumo de energía eléctrica y poca previsión de crecimiento.
Computadores y Laptops	4.33	Fenómenos naturales	Edificación no apropiada y poco segura.
		Amenaza Física	Mala coordinación de mantenimientos de equipos
		Robo de información relevante del negocio	Ausencia de políticas de contraseñas
		Caída del sistema por agotamiento de recursos	Cálculo inapropiado de consumo de energía eléctrica y poca previsión de crecimiento.
		Ataque de botnets	Revisión inadecuada de logs.
		Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.
		Amenaza lógica	Sistemas operativos mal configurados
Impresoras	5	Fenómenos naturales	Edificación no apropiada y poco segura.
		Amenaza Física	Mala coordinación de mantenimientos de equipos
		Ataques de Malware y Hackers	Mala administración de accesos físicos y lógicos.
		Worms maliciosos	Deficiente administración en tareas de impresión en la nube.
		Robo de información	No consideración de estos dispositivos en políticas de seguridad en redes.
		Caída del sistema por agotamiento de recursos	Cálculo inapropiado de consumo de energía eléctrica y no previsión de crecimiento.
		Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.
Tablet/Cámaras fotográficas	5	Fenómenos naturales	Edificación no apropiada y poco segura.
		Robo de información financiera	Escasa protección, anti virus específico para Tablets.
		Pérdida de datos	Administración descentralizada de dispositivos, que trae consigo la mala encriptación de transmisiones y datos expuestos ante posibles extravíos de dispositivos.
		Acceso remoto no autorizado	Inexistente cifrado de información y mala administración de contraseñas.
		Amenaza Física	Mala coordinación de mantenimientos de equipos
		Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.
Socios/ Auditores	5	Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.

		Robo de información relevante del negocio	Ausencia de políticas de contraseñas
		Ingeniería social	Mala difusión de políticas de seguridad.
		Malware	Ausencia de protección anti-malware para dispositivos móviles.
Personal administrativo	4.33	Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.
		Robo de información relevante del negocio	Ausencia de políticas de contraseñas
		Indisponibilidad del personal	Enfermedad
		Ingeniería social	Desconocimiento de políticas de seguridad
Sistema Integrado de Seguros	4	Malware	Base de datos de antivirus desactualizada
		Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo
		Cálculo de prima neta	Código de programación errado
		Operaciones no autorizadas	Deficiente administración de usuarios y permisos
		Cálculo de impuestos	Versiones desactualizadas
		Pérdida de información relevante del negocio	Respaldos incompletos
Software de Facturación	4.33	Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo
		Operaciones no autorizadas	Deficiente administración de usuarios y permisos
		Pérdida de información relevante del negocio	Respaldos incompletos
		Defectos y errores	Documentación técnica y operativa escasa o desactualizada
Software de Escaneo de documentos	4	Información desordenada	Ausencia de etiquetado (clasificación) de la información
		Pérdida de documentación	Ausencia de procedimientos de manejo de información clasificada
		Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo
		Operaciones no autorizadas	Deficiente administración de usuarios y permisos
		Pérdida de información relevante del negocio	Respaldos incompletos
		Defectos y errores	Documentación técnica y operativa escasa o desactualizada
Sitio web	3.33	Exposición de datos privados	Wifi Abierta y mala configuración de seguridad
		Robo de contraseñas	Ausencia de políticas de contraseñas

		Servicio inhabilitado	Falta de parcheo y revisiones de actualizaciones
Servicio de correo electrónico	4.66	Correo no deseado	Filtro inapropiado de spams
		Pérdida de información	Respaldos incompletos
		Servicio inhabilitado	Falta de parcheo y revisiones de actualizaciones
		Suplantación de identidad(spoofing)	Ausencia de revisiones periódicas de privilegios de acceso y comunicaciones inusuales
		Ataque de pishing o malware	Desconocimiento de políticas de seguridad
		Ataques de hombre en el medio	Deficiente encripta miento entre emisor y receptor
		Servicio inhabilitado	Agotamiento de recursos
Sistema de comunicación telefónica IP	4.33	Pérdida o robo de servicios	Escasa administración y monitoreo de puertos abiertos
		Caída del servicio	Piezas en mal estado desde su origen
		Operaciones no autorizadas	Deficiente administración de usuarios y permisos
Red de área local e inalámbrica	4	Robo de contraseña	Protocoles de seguridad antiguos.
		Malware	Puertas traseras activas, no detectadas
		Accesos no autorizados	Política de seguridad no adecuada
		Caída del servicio	Piezas en mal estado desde su origen
		Servicio inhabilitado	Agotamiento de recursos
		Operaciones no autorizadas	Deficiente administración de usuarios y permisos
Informes llenados durante el proceso	4.33	Información desordenada	Ausencia de etiquetado (clasificación) de la información
		Pérdida de documentación	Ausencia de procedimientos de manejo de información clasificada
		Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo
		Operaciones no autorizadas	Deficiente administración de usuarios y permisos
		Uso no previsto	Desconocimiento técnico
Papeles de Trabajo/Documentos físicos	4.33	Información desordenada	Ausencia de etiquetado (clasificación) de la información
		Pérdida de documentación	Ausencia de procedimientos de manejo de información clasificada
		Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo
		Operaciones no autorizadas	Deficiente administración de usuarios y permisos

3.6 CÁLCULO DE PROBABILIDAD DE LAS AMENAZAS

Luego de haberse determinado las amenazas y vulnerabilidades, se procederá con el cálculo de probabilidades. Para ello se tomará como referencia la tabla de probabilidad de ocurrencia de Magerit [4], así tenemos:

Tabla 5 Tabla de Probabilidad de Ocurrencia.
Fuente: Libro I MAGERIT PAG. 28

MA	100	MUY FRECUENTE	A DIARIO	5
A	10	FRECUENTE	MENSUALMENTE	4
M	1	NORMAL	UNA VEZ AL AÑO	3
B	1/10	POCO FRECUENTE	CADA VARIOS AÑOS	2
MB	1/100	MUY POCO FRECUENTE	SIGLOS	1

Para el nivel de aceptación del riesgo nos manejaremos con la tabla que se muestra a continuación:

Tabla 6 Niveles de Aceptación del Riesgo.

Niveles de Aceptación del Riesgo {E}		
Exposición al riesgo	Niveles	Objetivo
1 - 4	Aceptación	No aplica controles
5 - 10	Bajo	Aplica controles para llevar a nivel de aceptación
11 - 15	Medio	Aplica controles para llevar a nivel bajo
16 - 25	Alto	Aplica controles para llevar a nivel medio

[4] Tomado del Libro I MAGERIT PAG. 28

Tabla 7 Cálculo de Probabilidad de las Amenazas

Activo	Valor del Activo	PMAO	Amenaza	Vulnerabilidad asociada	P	VR	VRP
Servidores	5	4	Accesos no autorizados	Puertas traseras activas, no detectadas	3	15	**20**
			Ataques por denegación de servicio	Tecnología insuficiente u obsoleta	3	15	
			Robo de información relevante del negocio	Escasa administración y monitoreo de puertos abiertos	3	15	
			Configuraciones susceptibles de copia.	Regular administración de sistemas.	3	15	
			Fenómenos naturales	Edificación no apropiada y poco segura.	2	10	
			Amenaza Física	Mala coordinación de mantenimientos de equipos	3	15	
			Robo de contraseñas y permisos de archivos	Deficiente configuración de servicios no utilizados	3	15	
			Pérdida de información relevante del negocio	Respaldos incompletos	2	10	
			Acceso a privilegios de base de datos.	Parches inapropiados en equipos.	3	15	
			Amenaza lógica	No disponibilidad por falta de redundancia	2	10	
			Intrusiones a la red	Ausencia de políticas de contraseñas	3	15	
			Caída del sistema por agotamiento de recursos	Cálculo inapropiado de consumo de energía eléctrica y poca previsión de crecimiento.	2	10	
			Accesos no autorizados	Puertas traseras activas, no detectadas	3	15	
			Ataques por denegación de servicio	Tecnología insuficiente u obsoleta	4	20	
			Robo de información relevante del negocio	Escasa administración y monitoreo de puertos abiertos	3	15	
			Configuraciones susceptibles de copia.	Regular administración de sistemas.	3	15	
			Fenómenos naturales	Edificación no apropiada y poco segura.	4	20	
Computadores y Laptops	4.33	4	Fenómenos naturales	Edificación no apropiada y poco segura.	2	8.88	**17.32**
			Amenaza Física	Mala coordinación de mantenimientos de equipos	3	12.99	
			Robo de información relevante del negocio	Ausencia de políticas de contraseñas	3	12.99	
			Caída del sistema por agotamiento de recursos	Cálculo inapropiado de consumo de energía eléctrica y poca previsión de crecimiento.	2	8.66	
			Ataque de botnets	Revisión inadecuada de logs.	4	17.	

						32	
			Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.	3	12.99	
			Amenaza lógica	Sistemas operativos mal configurados	3	12.99	
Impresoras	5	4	Fenómenos naturales	Edificación no apropiada y poco segura.	2	10	**20**
			Amenaza Física	Mala coordinación de mantenimientos de equipos	3	15	
			Ataques de Malware y Hackers	Mala administración de accesos físicos y lógicos.	3	15	
			Worms maliciosos	Deficiente administración en tareas de impresión en la nube.	4	20	
			Robo de información	No consideración de estos dispositivos en políticas de seguridad en redes.	4	20	
			Caída del sistema por agotamiento de recursos	Cálculo inapropiado de consumo de energía eléctrica y no previsión de crecimiento.	2	10	
			Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.	2	10	
Tablets/Cámaras fotográficas	5	3	Fenómenos naturales	Edificación no apropiada y poco segura.	2	10	**15**
			Robo de información financiera	Escasa protección, anti virus específico para Tablets.	3	15	
			Pérdida de datos	Administración descentralizada de dispositivos, que trae consigo la mala encriptación de transmisiones y datos expuestos ante posibles extravíos de dispositivos.	3	15	
			Acceso remoto no autorizado	Inexistente cifrado de información y mala administración de contraseñas.	3	15	
			Amenaza Física	Mala coordinación de mantenimientos de equipos	2	10	
			Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.	3	15	
Socios/ Auditores	5	3	Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.	3	15	**15**
			Robo de información relevante del negocio	Ausencia de políticas de contraseñas	3	15	
			Ingeniería social	Mala difusión de políticas de seguridad.	3	15	
			Malware	Ausencia de protección anti-malware para dispositivos móviles.	3	15	
Personal administrativo	4.33	4	Uno inadecuado de equipo	Poco conocimiento en manejo de equipos.	3	12.99	**17.32**
			Robo de información relevante del negocio	Ausencia de políticas de contraseñas	3	12.99	
			Indisponibilidad del personal	Enfermedad	3	12.99	

			Emisión de pólizas erradas	Poco conocimiento de procedimientos y procesos	4	17.32	
			Ingeniería social	Desconocimiento de políticas de seguridad	3	12.99	
Sistema Integrado de Seguros	4	4	Malware	Base de datos de antivirus desactualizada	3	12	**16**
			Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo	4	16	
			Cálculo de prima neta	Código de programación errado	3	12	
			Operaciones no autorizadas	Deficiente administración de usuarios y permisos	3	12	
			Cálculo de impuestos	Versiones desactualizadas	3	12	
			Pérdida de información relevante del negocio	Respaldos incompletos	3	12	
Software de Facturación	4.33	4	Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo	4	17.32	**17.32**
			Operaciones no autorizadas	Deficiente administración de usuarios y permisos	3	12.99	
			Pérdida de información relevante del negocio	Respaldos incompletos	3	12.99	
			Defectos y errores	Documentación técnica y operativa escasa o desactualizada	3	12.99	
Software de Escaneo de documentos	4	4	Información desordenada	Ausencia de etiquetado (clasificación) de la información	3	12	**16**
			Pérdida de documentación	Ausencia de procedimientos de manejo de información clasificada	3	12	
			Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo	4	16	
			Operaciones no autorizadas	Deficiente administración de usuarios y permisos	3	12	
			Pérdida de información relevante del negocio	Respaldos incompletos	3	12	
			Defectos y errores	Documentación técnica y operativa escasa o desactualizada	3	12	
Sitio web	3.33	3	Exposición de datos privados	Wifi Abierta y mala configuración de seguridad	3	9.99	**9.99**
			Robo de contraseñas	Ausencia de políticas de contraseñas	3	9.99	
			Servicio inhabilitado	Falta de parcheo y revisiones de actualizaciones	3	9.99	
Servicio de correo electrónico	4.66	3	Correo no deseado	Filtro inapropiado de spams	3	13.98	**13.98**
			Pérdida de información	Respaldos incompletos	3	13.98	
			Servicio inhabilitado	Falta de parcheo y revisiones de actualizaciones	3	13.98	
			Suplantación de identidad(spoofing)	Ausencia de revisiones periódicas de privilegios de	3	13.98	

				acceso y comunicaciones inusuales			
			Ataque de pishing o malware	Desconocimiento de políticas de seguridad	3	13.98	
			Ataques de hombre en el medio	Deficiente encripta miento entre emisor y receptor	3	13.98	
			Servicio inhabilitado	Agotamiento de recursos	3	13.98	
Sistema de comunicación telefónica IP	4.33	3	Pérdida o robo de servicios	Escasa administración y monitoreo de puertos abiertos	3	12.99	**12.99**
			Caída del servicio	Piezas en mal estado desde su origen	3	12.99	
			Operaciones no autorizadas	Deficiente administración de usuarios y permisos	3	12.99	
Red de área local e inalámbrica	4	4	Robo de contraseña	Protocoles de seguridad antiguos.	4	16	**16**
			Malware	Puertas traseras activas, no detectadas	3	12	
			Accesos no autorizados	Política de seguridad no adecuada	3	12	
			Caída del servicio	Piezas en mal estado desde su origen	3	12	
			Servicio inhabilitado	Agotamiento de recursos	3	12	
			Operaciones no autorizadas	Deficiente administración de usuarios y permisos	3	12	
Informes llenados durante el proceso	4.33	4	Información desordenada	Ausencia de etiquetado (clasificación) de la información	3	12.99	**17.32**
			Pérdida de documentación	Ausencia de procedimientos de manejo de información clasificada	3	12.99	
			Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo	4	17.32	
			Operaciones no autorizadas	Deficiente administración de usuarios y permisos	3	12.99	
			Uso no previsto	Desconocimiento técnico	4	17.32	
Papeles de Trabajo/Documentos físicos	4.33	3	Información desordenada	Ausencia de etiquetado (clasificación) de la información	3	12.99	**17.32**
			Pérdida de documentación	Ausencia de procedimientos de manejo de información clasificada	3	12.99	
			Riesgo interno	Evaluación poco cuidadosa de la fuerza de trabajo	4	17.32	
			Operaciones no autorizadas	Deficiente administración de usuarios y permisos	3	12.99	

CAPÍTULO 4

PLAN DE TRATAMIENTO DE RIESGOS

4.1 INTRODUCCIÓN

Luego de haber realizado el análisis y cuantificación de los riesgos, es necesario realizar el plan de tratamiento de riesgos, mismo que consiste en seleccionar y aplicar controles adecuados con el único objetivo de modificar el riesgo y con ello evitar los daños a los que puede estar expuesta la organización.

El plan de tratamiento de riesgos debe asegurar como mínimo:

a) El funcionamiento eficiente y práctico de la empresa
b) La adopción de controles internos adecuados y
c) El seguimiento de las leyes y reglamentaciones actuales

Las medidas que se tomen para modificar, reducir o eliminar el riesgo contribuirán a mejorar el desempeño de la organización. Es por esta razón que dichos riesgos deben ser evaluados y cuantificados de acuerdo a su relevancia e importancia para la empresa.

Existen dos tipos de estrategias de riesgos, la primera es la estrategia de la evitación y la segunda la de minimización.

La estrategia de evitación busca minimizar la probabilidad de que el riesgo se haga presente, para ello se manejan cuatro opciones:

a) Transferir

Transferir es el conjunto de procedimientos que tiene como objetivo principal eliminar el riesgo transfiriéndolo de un lugar a otro, lo cual puede consistir en venderlo o asegurarlo.

b) Reducir

Reducir implica reducir las consecuencias que puede generar un riesgo, esto se logra implementando controles y procedimientos y asegurándonos que dichos controles y procedimientos se encuentren en el lugar apropiado

c) Eludir

Eludir conlleva dos opciones, la primera es no proceder con un determinado proyecto o actividad que permiten que el riesgo se materialice o seleccionar otros medios para realizar la actividad o proyecto.

d) Diversificar.

Diversificar consiste en extender el riesgo desde una determinada área hasta otros segmentos teniendo como finalidad impedir la pérdida de ingresos para la empresa.

La estrategia de minimización en cambio, busca reducir el impacto del riesgo que ya se ha materializado y por lo tanto se quiere tomar medidas para minimizar las consecuencias. Para esta estrategia es el Plan de Contingencia el que definirá procedimientos y las personas involucradas en dicho procedimiento.

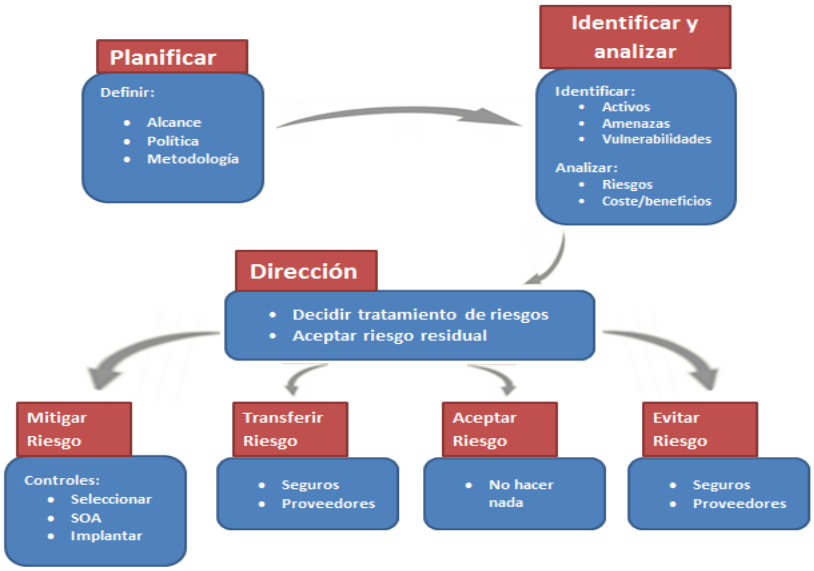


FIGURA 4.1 Opciones de tratamiento del riesgo. Fuente: ISO27001

4.2 BENEFICIOS PRÁCTICOS DE LA NORMA ISO 27001/2013

La norma ISO es utilizada por la flexibilidad y fácil adaptación a diferentes contextos. Ofrece además las mayores garantías para implementar el Sistema de Gestión de Seguridad de la Información, ya que ofrece cuatro pilares básicos como son:

a) Ordenamiento del negocio

b) Competitividad

c) Menores gastos y

d) Cumplimiento de las normas

En lo que se refiere al ordenamiento del negocio, este sucede cuando las empresas en busca de adaptarse a la norma ISO 27001 realizan actualizaciones y reestructuración ya sea de sus sistemas informáticos o de sus procesos,

ordenando para ello tanto a los responsables de cada proceso como sus recursos.

Al ser la norma ISO 27001 la base para el desarrollo e implementación del SGSI Sistema de Gestión de Seguridad de la información, este aspecto le otorga un valor añadido a la empresa en un mercado cada vez más enfocado a darle un mejor tratamiento a la información y por ello el grado de competitividad aumenta.

Aunque no existe de forma precisa como saber si existe una reducción de costos con el uso de esta norma, lo que sí es seguro es que al mejorar los procesos de gestión de datos y hacer un seguimiento a las evaluaciones y soluciones, se logra con la ayuda del SGSI a enfocarse en la prevención y con ello mejorar las finanzas.

En lo que se refiere al cumplimiento de las normas, la norma ISO 27001 ayuda a revisar el grado de cumplimiento con las legislaciones vigentes y otorga las soluciones que pueden ser consideradas para una adecuada actualización, por ello es muy utilizada en organizaciones financieras, de salud o de carácter gubernamental.

Además de los cuatro beneficios indicados anteriormente en referencia a esta norma, hay otros que vienen por añadidura como son:

a) Creación de bancos de datos
b) Credibilidad y confianza
c) Disminución de incidentes informáticos
d) Sensibilización del personal en torno a la seguridad informática

4.3 IMPLEMENTACIÓN DE CONTROLES

Aunque es importante para la empresa que sus operaciones sean realizadas sin interrupciones, es preciso indicar que eliminar el riesgo completamente es casi imposible, más sin embargo es posible entrenar al equipo de trabajo de tal forma que puedan detectar debilidades y con ello evitar posibles incidentes de seguridad

Los incidentes pueden ser diferentes y por ello es importante comunicar cualquier cambio en el estado del mismo.

FIGURA 4.2 Gestionar incidentes de seguridad basado en la norma ISO 27001

La gestión de incidentes de seguridad basados en la norma ISO 27001 se logra tomando en consideración las siguientes medidas:

a) Notificando los incidentes que puedan generar algún evento negativo para la organización, utilizando para ellos los procedimientos establecidos.
b) Clasificando los incidentes de tal forma que puedan ser diferenciados de acuerdo a su nivel de riesgo para la organización.
c) Tratando los riesgos, estableciendo el tiempo que tendrá para ser resuelto y las medidas que serán tomadas.
d) Cerrar los incidentes de tal forma que toda la información en referencia quede registrada, incluyendo el aviso de cierre del incidente a la persona que notificó el incidente, y,

e) Creando una base de datos con los conocimientos necesarios del incidente, como fue tratado y su nivel de perjuicio para la organización.

En todo caso es importante que todos los controles que puedan ser aplicables a un evento que pueda llegar a afectar o dañar las operaciones de la organización, sirvan para garantizar el cumplimiento de medidas, procedimientos y políticas que ayuden a mitigar un determinado riesgo.

La norma ISO 27001:2013 cuenta con los controles especificados en el anexo A, mismo que proporciona catorce categorías de control (del 5 al 18), que sirven como base de referencia desde donde se pueden extraer los controles necesarios de acuerdo a la necesidad que requiera ser cubierta. Entre estos controles tenemos:

a) Políticas de la seguridad de la información
b) Organización de la seguridad de la información
c) Seguridad de los Recursos Humanos
d) Gestión de activos
e) Control de acceso
f) Criptografía
g) Seguridad física y del entorno
h) Seguridad de las operaciones
i) Seguridad de las comunicaciones
j) Adquisición, desarrollo y mantenimiento de sistemas
k) Relaciones con los proveedores
l) Gestión de incidentes de seguridad de la información
m) Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

n) Cumplimiento

4.4 TRATAMIENTO DEL RIESGO

La implementación de controles como una forma de mitigar el riesgo se puede hacer en base a lo que recoge el Anexo A de la norma ISO 27001. Después de realizar el análisis y la evaluación del riesgo, se debe pensar en las acciones que deben tomarse para todos aquellos activos que están a expensas de sufrir una eventual amenaza. Motivo por el cual los controles o procedimientos que se asignen para cada uno de ellos deben ir acorde con las políticas de seguridad existentes o que se encuentren en fase de implementación, ya que las mismas constituyen nuestro respaldo para mitigar y controlar los riesgos que se puedan presentar.

Una vez que el riesgo se ha calculado, se debe iniciar un proceso de toma de decisiones con respecto al tratamiento del riesgo basado en:

- Los activos que se encuentran más expuestos
- El impacto y degradación que puede causar
- La frecuencia con la que puede ocurrir.

Es aquí donde nos damos cuenta de la importancia que tiene la clasificación e identificación de los activos, ya que una amenaza se puede activar para todos o solo para alguno de ellos, por lo que resulta importante identificar dichas amenazas para reducirlas o eliminarlas. La empresa debe evaluar cuales son las opciones de tratamiento de riesgo y decidir los objetivos de control y controles que se escogerán para dicho tratamiento. La aceptación del riesgo juega un papel importante ya que establece un criterio para la selección de controles de acuerdo a las normas legales vigentes tanto de entes reguladores como de

entornos legales. La norma indica en la cláusula 4.2.1 que se refiere a Establecer el SGSI, que dichos controles deben ser considerados a partir del Anexo A.

El Anexo A nos provee de una serie de delineamientos que nos permiten evaluar y tomar una acción preventiva para aquellos riesgos que se identificaron con anterioridad y de esta forma escoger una estrategia de tratamiento de riesgos adecuada de acuerdo a la necesidad del negocio. La identificación de dichos riesgos se base en el análisis realizado de acuerdo a la importancia de cada activo para las operaciones que el negocio debe realizar y cada valoración que se le haya asignado. A continuación, se muestra el plan de tratamiento para los activos, tomando como base su clasificación general, tales como: Hardware, Persona, Software/Información, Servicio, Comunicaciones y Datos/Soportes, así como también los controles aplicados tomando como base la norma ISO 27001-2013, la codificación de Magerit para el enlista miento de las amenazas y la opción de tratamiento de riesgos.

Tabla 8 Tratamiento de Riesgos: Hardware Fuente: Autor

Activos de Información	Responsable de Activo	Amenazas	Vulnerabilidades	Opciones de Tratamiento del riesgo	
				Opción de Tratamiento de Riesgo	Controles o Salvaguardas
Hardware: Servidores, Computadores, Laptops,	Jefe TI	[N.1] Incendio	• N.1.1 Escaso equipo contra incendios. • N.1.2 Mala política de escritorio limpio. • N.1.3 No cumplimiento de reglamento interno en lo que se refiere a normas de buena conducta. • N.1.4 Fallo en revisión de conexiones eléctricas	Reducción	• A.6.1.3 Contacto con autoridades **(N.1.1)** • A.9.1.1 Política de control de acceso **(N1.1)** • A.11.1.4 Protección contra amenazas externas y ambientales **(N.1.1, N.1.3,**
		[N.2] Inundación	• N.2.1 Sistema de climatización sin mantenimiento.		

			• N.2.2 Mala disposición de tuberías de pisos superiores		**N.2.1, N.2.2, I.6.1,I.7.1,N.3)** • A.11.2.1 Instalación y protección de equipos (**I.6.1,I.7.1)** • A.11.2.9 Política de pantalla y escritorio limpio **(N.1.2)** • A.11.2.3 Seguridad del cableado **(N.1.4)** • A.11.2.4 Mantenimiento de equipos **(I.6.1, E.23.1, E.2.1, I.5.1, A.23.2)** • A.11.2.8 Equipos de usuario desatendido**(A.23.2)** • A.8.1.2 Propiedad de los activos**(A.23.1)** • A.8.1.3 Uso aceptable de equipos**(A.23.1)** • A.9.1.1 Política de control de acceso**(A.7.1)** • A.8.1.1 Inventario de equipos**(E.25.1)** • A.9.4.2 Procedimiento de acceso seguro**(E.15.1,E.18.1)** • A.12.3.1 Respaldo de información**(E.15.1,E.18.1)**
		[N.*] Desastres naturales	• N.3.1 Diseño antisísmico no adecuado.		
		[I.7] Condiciones inadecuadas de temperatura o humedad	• I.7.1 Deficiencia en la climatización		
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	• E.23.1 Desconocimiento de procedimientos o controles de actualización de equipos.		
		[I.6] Corte del suministro eléctrico	• I.6.1 Falla en mantenimiento de UPS.		
		[E.2] Errores del administrador	• E.2.1 Desconocimiento en instalación de equipos		
		[A.7] Uso no previsto	• A.7.1 Perfiles de seguridad no establecidos		
		[A.23] Manipulación de los equipos	• A.23.1 Sabotaje de hardware por falla en políticas de administración de equipos. • A.23.2 Mala administración de mantenimiento de equipos. • A.23.2 Overflow por falta de verificación de capacidades del equipo		
		[I.5] Avería de origen físico o lógico	• I.5.1 Fallos en los equipos por defecto de origen		
		[E.15] Alteración accidental de la información	• E.15.1 Alteración accidental de datos sobre todo en los recabados por dispositivos tales como: Tablets o cámaras		
		[E.18] Pérdida accidental de la información	• E.18.1 Pérdida accidental de información sobre todo en dispositivos tales como: Tablets o cámaras.		
		[E.25] Pérdida de equipos	• E.25.1 Insuficiente control de manejo de inventarios		

Tabla 9 Tratamiento de Riesgos: Personas Fuente: Autor

Activos de Información	Responsable de Activo	Amenazas	Vulnerabilidades	Opciones de Tratamiento del riesgo	
				Opción de Tratamiento de Riesgo	Controles o Salvaguardas
Personas: Socios, Auditores, Personal Administrativo	Gerente General y Oficial de Cumplimiento	[E.28] Indisponibilidad del personal (no intencionado)	• E.28.1 Enfermedad • E.28.2 Alteraciones en el orden publico	Reducción	• A.6.1.3 Contacto con autoridades **(E.28.2)** • A.11.1.4 Protección contra amenazas externas y ambientales**(E.28.2)** • A.6.1.2 Separación de deberes **(E.28.1)** • A.11.2.8 Equipos de usuario desatendido **(A.40.1)** • A.11.2.9 Política de escritorio limpio y pantalla limpia **(A.40.2)** • A.18.1.4 Privacidad y protección de información de datos personales **(A.40.1)** • A.18.1.3 Protección de registros **(A.40.2)** • A.6.2.1 Política para dispositivos móviles **(A.40.3)** • A.5.1.1 Políticas para la seguridad de la información**(A.30.1, A.30.2, A.5)** • A.6.1.1 Roles y responsabilidades para la seguridad de la información**(A.30.2, A.5)** • A.9.2.1 Gestión de derechos de
		[A.40] Intrusión en privacidad personal	• A.40.1 Publicación de datos personales en redes virtuales de Internet • A.40.2 Documentos con datos personales en los escritorios • A.40.3 Ausencia de contraseñas en teléfonos inteligentes		
		[A.30] Ingeniería social	• A.30.1 Mala difusión de políticas de seguridad. • A.30.2 Roles de seguridad no asignados o comunicados • A.30.3 Escaso control ante ataques de malware o pishing.		
		[A.11] Acceso no autorizado	• A.11 Fallo del sistema en la identificación y autorización		
		[E.7] Deficiencias en la organización	• E.7.1 Acciones no coordinadas • E.7.2 Errores por omisión • E.7.3 Roles mal definidos • E.7.4 Desconocimiento de procedimientos		
		[E.1] Errores de los usuarios	• E1.1 Mala difusión de políticas de seguridad. • E1.2 Roles de seguridad no asignados o comunicados • E1.3 Empoderamiento inexistente en lo que se refiere a políticas de seguridad • E1.4 Personal con tareas rutinarias		
		[E.19] Fugas de información	• E.19.1 Revelación de información por indiscreción ya sea verbalmente, medios electrónicos o papel.		
		[A.5] Suplantación de identidad del usuario	• A.5.1 Privilegios y accesos pobres para acceso a equipos.		

		[A.6] Abuso de privilegios de acceso	• A.6.1 Mala definición de privilegios en tareas que realizan los usuarios.		acceso privilegiado**(A.6)** • A.9.3.1 Uso de información de autenticación secreta**(E.19)** • A.13.2.3 Mensajería electrónica**(A.30.3)** • A.13.2.4 Acuerdos de confidencialidad y no divulgación**(A.30.3)** • A.18.2.2 Cumplimiento en las políticas y normas de seguridad**(E.7,E1,A.7,A.6)** • A.10.1.1 Política sobre uso de controles criptográficos**(A.40,A.30.3,A.11)** • A.7.1.2 Términos y condiciones del empleo**(A.5)** • A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información**(A.5,A.6,A.7)**
		[A.7] Uso no previsto	• A.7.1 Uso de recursos del sistema para temas de interés personal.		

Tabla 10 Tratamiento de Riesgos: Software Fuente: Autor

Activos de Información	Responsable de Activo	Amenazas	Vulnerabilidades	Opciones de Tratamiento del riesgo	
				Opción de Tratamiento de Riesgo	Controles o Salvaguardas
Software /Información: Sistema Integrado de Seguros, Software de Facturación, Software de escaneo de documentos	Jefe de TI	[I.5] Avería de origen físico o lógico	• I.5.1 Fallo en los programas • I.5.2 Acceso no permitido	Reducción	• A.7.1.2 Términos y condiciones del empleo **(A.5)** • A.9.1.2 Acceso a redes y a servicios de red **(E.8)** • A.9.2.3 Gestión de derecho de acceso privilegiado **(E.8, A.5,E.15)** • A.9.2.4 Gestión de información de autenticación secreta de usuarios **(I.5.2, E.19,A.5)** • A.9.3.1 Uso de información de autenticación secreta **(I.5.2, E.19,A.5)** • A.9.4.1 Restricción de acceso a la información **(I.5, E.1)** • A.9.4.5 Control de acceso a códigos fuentes de programas**(I.5, E.20,E.21)** • A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación**(I.5,E.20,E. 21)** • A.14.2.7 Desarrollo contratado externamente **(I.5, E.21,E.20)** • A.14.2.8 Pruebas de seguridad de sistemas **(I.5, E.21,E.20)** • A.12.3.1 Respaldo de la información **(E.18)**
		[E.1] Errores de los usuarios	• E.1.1 Error en ingreso de datos • E.1.2 Errores de uso del sistema		
		[E.8] Difusión de software dañino	• E.8.1 Propagación no intencional de virus		
		[E.15] Alteración accidental de información	• E.15.1 Desconocimiento del procedimiento • E.15.2 Pobre inducción del sistema		
		[E.18] Destrucción de información	• E.18.1 Pérdida accidental de información		
		[E.19] Fuga de información	• E.19.1 Revelación de información por indiscreción ya sea verbalmente, medios electrónicos o papel.		
		[E.20] Vulnerabilidad de los programas	• E.20.1 Defectos del código • E.20.2 Operación errónea		
		[E.21] Errores de mantenimiento y actualización de programas	• E.21.1 Procedimientos y controles ineficientes para pase de programas a producción. • E.21.2 Procedimientos y controles ineficientes para revisiones de software contratado externamente. • E.21.3 No cumple con reglas del negocio		
		[A.5] Suplantación de identidad del usuario	• A.5.1 Desconocimiento por parte del personal de las políticas de seguridad • A.5.2 Desconocimiento de responsabilidades en referencia a la labor que realiza. • A5.3 Contraseñas débiles - fáciles de averiguar		

Tabla 11 Tratamiento de Riesgos: Servicios Fuente: Autor

Activos de Información	Responsable de Activo	Amenazas	Vulnerabilidades	Opciones de Tratamiento del riesgo	
				Opción de Tratamiento de Riesgo	Controles o Salvaguardas
Servicio: Sitio WEB, Servicio de correo electrónico	Jefe de TI	[A.7] Uso no previsto	• A.7.1 Equivocación de usuarios • A.7.2 Equivocación de administrador • A.7.3 Mala difusión de políticas	Reducción	• A.9.1.1 Política de control de acceso **(A.7, N.1.1)** • A.18.2.2 Cumplimiento en las políticas y normas de seguridad **(A.7)** • A.6.1.3 Contacto con autoridades **(N.1.1)** • A.11.1.4 Protección contra amenazas externas y ambientales **(N.1.1, N.1.3, N.2, I.6.1,I.7.1,N.3,I*)** • A.11.2.9 Política de pantalla y escritorio limpio **(N.1.2)** • A.11.2.3 Seguridad del cableado **(N.1.3,I*)** • A.9.2.5 Revisión de los derechos de acceso de usuarios **(A.4.2)** • A.9.3.1 Uso de información de autenticación secreta **(A.5)** • A.9.4.3 Sistema de control de contraseñas **(A.5, A.4.2)** • A.11.2.2 Servicio de suministro **(I.6)** • A.11.2.4 Mantenimiento de
		[E.24] Servicio inhabilitado	• E.24.1 Recursos escasos o mal definidos • E.24.2 Mala administración de privilegios de accesos. • E.24.3 Ejecución de instrucciones no previstas. • E.24.4 Errores de configuración • E.24.5 Tareas programadas con protección inadecuada. • E.24.6 Enlace de internet caído. • E.24.7 Utilización de código abierto no probado. • E.24.8 Malware/Spam		
		[N.1] Incendio	• N.1.1 Escaso equipo contra incendios. • N.1.2 Mala política de escritorio limpio • N.1.3 Fallo en revisión de conexiones eléctricas		
		[N.2] Inundación	• N.2.1 Sistema de climatización sin mantenimiento. • N.2.2 Mala disposición de tuberías de pisos superiores.		
		[N.*] Desastres naturales	• N.3.1 Diseño antisísmico no adecuado.		
		[I.*] Daño eléctrico	• I.1.1 Aumento o disminución de voltajes no controlados. • I.1.2 Sobrecarga de regletas o tomacorrientes. • I.1.3 Mala política de escritorio limpio		
		[I.5] Fallas de origen físico	• I.5.1 Desactualizaciones, incompatibilidad de versiones. • I.5.2 Inducción inadecuada		

			para manejo de equipos. • I.5.3 Desgaste o desactualización de componentes • I.5.4 Piezas en mal estado desde su origen. • I.5.5 Sistema de climatización si mantenimiento. • I.5.6 Falta de mantenimiento o soporte físico. • I.5.7 Componentes mal instalados o conectados.		equipos **(I.5)** • A.11.2.8 Equipos de usuario desatendido **(E.24)** • A.12.2.1 Controles de código malicioso **(E.24)** • A.12.4.1 Registro de eventos **(A.4.1)** • A.13.2.3 Mensajería electrónica **(E.24,A.5)** • A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos de los proveedores **(E.24)** • A.18.2.3 Revisión del cumplimiento técnico **(A.7, E.24, A.4, A.5)**
		[I.6] Corte prolongado de suministro eléctrico	• I.6.1 Racionamientos • I.6.2 Trabajos prolongados en redes eléctricas externas		
		[A.4] Manipulación de la configuración	• A.4.1 Inexperiencia en administración de configuración • A.4.2 Auditorías deficientes a la red.		
		[A.5] Suplantación de la identidad del usuario	• A.5.1 Mala difusión de políticas de seguridad. • A.5.3 Mala disposición de enlaces adecuados a la página.		

Tabla 12 Tratamiento de Riesgos: Comunicaciones Fuente: Autor

Activos de Información	Responsable de Activo	Amenazas	Vulnerabilidades	Opciones de Tratamiento del riesgo	
				Opción de Tratamiento de Riesgo	Controles o Salvaguardas
Comunicaciones: Sistema de Comunicación Telefónica IP y Red de Área Local e Inalámbrica	Jefe de TI	[E.15] Alteración accidental de la información	• E.15.1 Configuración incorrecta del sistema de archivos. • Incorrecta administración de perfiles y grupos de acceso.	Reducción	• A.5.1.1. Políticas para la seguridad de la información **(E.15, E.18, A.5, A.7)** • A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información **(A.7.1, E.19)** • A.9.4.3 Sistema de control de contraseñas **(A.5, A.4.2)** • A.11.2.8 Equipos de usuario desatendido **(E.24)** • A.12.2.1 Controles de código malicioso **(A.11)** • A.9.2.5 Revisión de los derechos de acceso de usuarios **(E.15, E.18, E.19,A.5,A.11)** • A.12.3.1 Respaldo de la información **(E.18)**
		[E.18] Destrucción de información	• E.18.1 Intrusión no esperada • E.18.2 Mantenimiento inapropiado de la red.		
		[E.19] Fugas de información	• E.19.1 Revelación por indiscreción		
		[E.24] Caída del sistema por agotamiento de recursos	• E.24.1 Recursos insuficientes para la carga de trabajo establecida		
		[A.5] Suplantación de la identidad del usuario	• A.5.1 Mala difusión de políticas de seguridad • A.5.3 Ataques IP spoofing / DNS spoofing.		
		[A.11] Acceso no autorizado	• A.7.1 Utilización para fines personales • A.7.2 Falla en control de privilegios. • A.7.3 Política de seguridad ineficiente • A.7.4 Debilidad en el diseño del protocolo utilizado • A.7.5 Existencia de puertas traseras • A.7.6 Descuido de los fabricantes		

Tabla 13 Plan de Tratamiento del riesgo: Soporte Fuente: Autor

Activos de Información	Responsable de Activo	Amenazas	Vulnerabilidades	Opciones de Tratamiento del riesgo	
				Opción de Tratamiento de Riesgo	Controles o Salvaguardas
Datos/Soportes de Información: Informes llenados durante proceso, Papeles de trabajo documentos físicos	Gerente de Operaciones, Gerente Técnico y Oficial de Riesgos	[N.1] Incendio	• N.1.1 Escaso equipo contra incendios. • N.1.2 Mala política de escritorio limpio. • N.1.3 No cumplimiento de reglamento interno en lo que se refiere a normas de buena conducta.	Reducción	• A.9.1.1 Política de control de acceso **(A.7, N.1.1)** • A.18.2.2 Cumplimiento en las políticas y normas de seguridad **(A.7)** • A.6.1.3 Contacto con autoridades **(N.1.1)** • A.11.1.4 Protección contra amenazas externas y ambientales **(N.1.1, N.1.3, N.2, N.*,A.26, I.3, I.7)** • A.11.2.9 Política de pantalla y escritorio limpio **(N.1.2)** • A.17.1.1 Planificación de la continuidad de la seguridad de la información **(A.7, I.9)** • A.18.1.3 Protección de registros **(A.7)** • A.5.1.1 Políticas para la seguridad de la información **(A.7, I.9, A.18)**
		[N.2] Inundación	• N.2.1 Sistema de climatización sin mantenimiento. • N.2.2 Mala disposición de tuberías en pisos superiores.		
		[N.*] Desastres naturales	• N.3.1 Diseño antisísmico no adecuado.		
		[I.3] Contaminación mecánica	• I.3.1 Mala disposición y almacenamiento de documentos. • I.3.2 Control de perímetro de acceso incierto.		
		[A.18] Destrucción de información	• A.18.1 Ausencia de etiquetado (clasificación) de la información		
		[I.7] Condiciones inadecuadas de temperatura o humedad	• I.7.1 Sitios de almacenamiento desprotegidos		
		[I.9] Interrupción de otros servicios y suministros esenciales	• I.9 No disponibilidad de recursos de los cuales depende la operación, como papel o tóner.		
		[A.7] Manipulación de documentación.	• A.7.1 Deficiente manejo de información clasificada • A7.2 Mala difusión de políticas de seguridad. • A.7.3 Documentación con fallas estructurales no acordes a la organización		

Tabla 14 Tabla de Responsabilidades

Áreas	Rol	Responsabilidades
Sistemas	Jefe de Sistemas	✓ Planear, organizar, Dirigir y Controlar, el funcionamiento del Área de Sistemas. ✓ Determinar normas y procedimientos del uso de Hardware y Software. ✓ Coordinar la atención y resolución de problemas y requerimientos ✓ Evaluar e identificar los riesgos informáticos que pueden llegar a amenazar la continuidad del negocio. ✓ Trabajar en conjunto con la Gerencia General para clarificar los riesgos del negocio y diseñar planes de acción. ✓ Garantizar la disponibilidad de los sistemas. ✓ Implementar procedimientos para la recuperación del sistema en caso de fallos. ✓ Diseñar en conjunto con la Gerencia General el DRP de acuerdo a los riesgos que se encuentra expuesto el negocio. ✓ Alinear la estrategia de tecnologías de la información con las del negocio.
Técnico	Gerente Técnico	✓ Trabajar en conjunto con la Gerencia General en el plan estratégico de la Compañía de Seguros. ✓ Proponer políticas y procedimientos para la Gestión Integral de Riesgos. ✓ Promover cultura organizacional de riesgos. ✓ Controlar las operaciones técnicas y operativas. ✓ Optimizar procesos de gestión en áreas operativas. ✓ Coordinar las actividades del proceso técnico de Cotización y Suscripción de la póliza. ✓ Promover entre su equipo de trabajo buenas prácticas en materia de gestión de documentos y archivos. ✓ Controlar las operaciones de las áreas técnica y operativa para lograr un buen funcionamiento de la Compañía. ✓ Asesorar y atender la renovación de pólizas de clientes importantes. ✓ Coordinar las inspecciones de riesgo en los casos que considere necesario efectuarlas o cuando los reaseguradores

		así lo soliciten. ✓ Colaborar con el área de Operaciones para dar cumplimiento a lo dispuesto por la empresa. ✓ Velar por el cumplimiento de los procedimientos técnicos, según las condiciones de los contratos de seguros.
Operaciones	Gerente Operaciones	✓ Trabajar en conjunto con la Gerencia General en el plan estratégico de la Compañía de Seguros. ✓ Proponer políticas y procedimientos para la Gestión Integral de Riesgos. ✓ Buscar la integración entre los planes de negocio y la gestión integral de riesgos. ✓ Desarrollar controles apropiados para dar soporte a la continuidad del negocio. ✓ Informar a la Gerencia General de forma oportuna los aspectos más importantes de la gestión de riesgos. ✓ Monitorear el cumplimiento de las políticas y delineamientos establecidos para la continuidad del negocio. ✓ Promover cultura organizacional de riesgos. ✓ Supervisar y controlar la ejecución de las políticas, normas y procedimientos establecidos para la suscripción de los ramos que maneja la empresa.
Dirección General	Gerente General	✓ Diseñar y presentar el Manual de Riesgo Operativo para su aprobación por parte del Comité General. ✓ Velar por el cumplimiento de las medidas establecidas por el Comité General. ✓ Velar para que la administración del riesgo operativo sea llevada a cabo mediante la correcta implementación de procedimientos. ✓ Aprobar los planes de contingencia y de continuidad del negocio. ✓ Procurar que el registro de eventos de riesgos operativos cumplan con la disponibilidad, integridad y confiabilidad. ✓ Evaluar informes remitidos por los órganos de control.
Unidad de Cumplimiento	Oficial de cumplimiento	✓ Definir procedimientos para prevenir y controlar el lavado de activos ✓ Realizar investigación de mercado para conocer los segmentos en que se encuentra dividido. ✓ Reportar las faltas o errores en cuanto a responsabilidades de los funcionarios.

		✓ Realizar el seguimiento de operaciones inusuales. ✓ Trabajar en conjunto con la Gerencia General para definir política de conocimiento al cliente. ✓ Verificar que la entidad aplique los instrumentos necesarios para alcanzar el conocimiento del mercado en que sus clientes desarrollan su actividad comercial. ✓ Verificar los datos suministrados por los clientes y que estos sean actualizados de forma periódica a medida que sean requeridos por la compañía de seguros.
Operaciones	Ejecutivo de Operaciones	✓ Revisar solicitudes de emisión y análisis en base a políticas de suscripción ✓ Procesar las renovaciones, movimientos nuevos y endosos de pólizas. ✓ Llevar un control y seguimiento a los folios asignados por el Gerente de Operaciones por trámite u orden de trabajo. ✓ Administrar el proceso de emisión y armado para garantizar el cumplimiento en tiempos de emisión y estándares de servicio establecidos por convenio ✓ Cumplir con las políticas de seguridad de la empresa. ✓ Cumplir con las políticas y delineamientos establecidos para la continuidad del negocio. ✓ Adoptar la cultura organizacional de riesgos indicada por la empresa.
Unidad de Riesgos	Oficial de riesgos	✓ Definir procedimientos y métodos para la correcta administración del riesgo operativo. ✓ Implementar y definir reportes internos y externos concernientes al riesgo operativo de la entidad. ✓ Crear modelos de medición de riesgo. ✓ Promover una adecuada gestión de continuidad del negocio. ✓ Colaborar con actividades dirigidas a procesos de control interno. ✓ Gestionar periódicamente reportes sobre la gestión de continuidad.
Comercial	Gerente Comercial	✓ Alinear su estrategia con la política dictada por el directorio y busca la mejor manera de alcanzar los objetivos y metas planteados. ✓ Supervisar el trabajo del equipo. ✓ Definir y dirigir la estrategia comercial. ✓ Analizar y desarrollar productos y

		servicios ✓ Coordinar la renovación de clientes.
Comercial	Ejecutivo Comercial	✓ Coordinar con la gerencia Comercial la ejecución de metas y objetivos. ✓ Atender los requerimientos y solicitudes de seguros de los clientes ✓ Gestionar las cotizaciones para su presentación y aprobación por el cliente. ✓ Controlar el Vencimiento de Pólizas, mediante mails, cartas o comunicados. ✓ Presentar a la Gerencia Comercial un reporte mensual de las pólizas por vencer a fin de determinar las estrategias más convenientes para cierre de las renovaciones

Una vez establecidos los parámetros para el tratamiento adecuado de los riesgos, es importante recordar que no es posible bloquear todas las amenazas a las que los activos puedan estar expuestos. Por lo que es preciso considerar que siempre existirá un riesgo residual, es decir aquel que aún persiste después de haber aplicado todos los controles sugeridos. Es preciso por ello establecer un conjunto de acciones encaminadas a mitigar este tipo de riesgo y que permita agilitar la toma de decisiones en el caso de que llegare a ocurrir un evento que pueda perjudicar a los activos de la organización y con ello a sus operaciones. No debemos perder de vista este riesgo y por ello es necesario que se establezcan políticas y procedimientos claros que ayuden a minimizar o reducir la ocurrencia de los mismos.

La reducción de los riesgos viene de la mano con una inversión de tipo económica por lo que muchas empresas o negocios optan por aceptarlo. Esta aceptación implica su documentación y registro, así como también la respectiva comunicación a la más alta autoridad del negocio, para que esté consiente ante cualquier eventualidad que pueda llegar a suceder. Por lo demás el Anexo A de

la norma ISO: 27001 nos ofrece los controles que deben ser tomados en cuenta durante la elaboración del SGSI.

CAPÍTULO 5

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

5.1 DEFINICIÓN DE POLÍTICAS

Las políticas o normas de seguridad son adoptadas por las empresas con la finalidad de mitigar posibles amenazas que pueden aparecer durante el ciclo de sus diferentes procesos y con ello proteger al activo más importante que es la información y a los sistemas que la tratan, debe además contemplar los elementos claves de seguridad tales como: la integridad, disponibilidad y confidencialidad.

La definición de estas políticas requiere un alto compromiso, así como también constancia y responsabilidad por parte de la organización y deben por lo tanto ser fáciles de lograr y de entender y estar lo más apegadas posible a la realidad de la misma. El departamento de TI y el departamento de Riesgos tienen a su cargo la implementación del Manual de Políticas de seguridad debido a que entre sus funciones están:

- Gestión de proyectos para soportar los requerimientos del negocio.
- Evaluación de hardware y software requerido por el negocio.
- Administración de recursos tecnológicos y plataformas que lo soportan.
- Gestión de los incidentes de seguridad de la información encontrados.
- Garantizar que se cumplan los principios básicos de seguridad como son: integridad, confidencialidad y disponibilidad de la información.

5.2 POLÍTICAS PROPIAS DEL NEGOCIO

5.2.1 POLÍTICAS DE SUSCRIPCIÓN

- Aceptar riesgos que pertenezcan a ramos de los cuales se tiene los suficientes conocimientos técnicos.
- Recabar información suficiente en referencia al riesgo que se desea aceptar.
- Aceptar riesgos que no lleguen a afectar la reputación de la empresa.
- Aceptar riesgos que no tengan como único fin el aseguramiento de solo y exclusivamente coberturas de tipo catástrofes.
- Aceptar riesgos que no se relacionen con actividades donde se trate con asbesto o temas nucleares.
- Cotizar las primas previendo que cubran los siniestros previstos y gastos de adquisición, así como también los costos de capital, de reaseguro e internos.
- Ceñir el contenido de la póliza de acuerdo a lo dispuesto en la legislación sobre el contrato de seguro constante en el Código de Comercio, el decreto supremo No. 1147 publicado en el Registro Oficial

No. 123 de 7 de diciembre de 1963, a la presente Ley y a las demás disposiciones que fueren aplicables.

- Redactar la póliza de forma clara para el asegurado.
- Incluir el listado de documentos básicos necesarios para la reclamación de un siniestro.
- Figurar las coberturas básicas y las exclusiones con caracteres destacados en la póliza.

5.2.2 POLÍTICAS DE REASEGURO

- Contratación de reaseguro con entidades de demostrada solvencia.
- Mantener un expediente actualizado con la información del reasegurador o reaseguradores que intervienen en el contrato, así como sus exclusiones, límites, deducibles, porcentajes de participación y cláusulas convenidas.
- Alinear los contratos automáticos de acuerdo a las condiciones, formas y métodos generalmente aceptados en la práctica internacional y se sujetarán a las disposiciones establecidas en la Ley General de Seguros, en el Reglamento General a la Ley General de Seguros.

5.2.3 POLÍTICAS DE EMISIÓN DE PÓLIZAS

- Cumplir con llenado de documento de conozca a su cliente
- Cumplir con la revisión de los datos del cliente en referencia a la base entregada por la Unidad de Análisis y Control Financiero.
- Cumplir con la inspección del riesgo asegurable.

- Asignar personal con el suficiente conocimiento técnico tanto para la cotización del seguro como para la emisión del mismo.
- Informar al cliente sobre el valor del seguro de acuerdo a la inspección realizada
- Presentar al cliente de forma clara y precisa las coberturas, cláusulas y condiciones, así como también valores en referencia a: primas, impuestos y deducibles relacionados con el contrato del seguros.
- Garantizar que todo bien asegurado tenga el respaldo de un reaseguro
- Garantizar que la póliza no tenga errores de definición o estructural.
- Garantizar que los valores cobrados a nivel de prima e impuestos sean correctos y respalden la eventualidad de ocurrencia de un siniestro.
- Garantizar la entrega de cotizaciones al cliente y/o bróker de negocios a renovarse considerando como mínimo un mes de anticipación.
- Garantizar que las cotizaciones a procesarse pertenezcan a clientes que han sido objeto de estudio, tanto a nivel de sus siniestros, como de su cartera y datos requeridos para la Unidad de Lavado de Activos.

5.3 POLÍTICAS GENERALES

- Los activos entregados a los empleados para la ejecución de sus labores son propiedad de la compañía. El uso de estas herramientas sean de hardware o de software debe estar estrictamente relacionados con el trabajo asignado.
- Cada individuo está autorizado para acceder a la información inherente con las actividades que realiza.

- Considerando los accesos otorgados por TI, cada individuo tendrá acceso sola y únicamente a las actividades conectadas para el usuario creado.
- La información de los sistemas deberá estar siempre disponible para asuntos del negocio.
- Debe haber una separación real de autoridad y responsabilidad para asegurar que ningún individuo tiene control exclusivo de una pieza de información.
- Las medidas de seguridad deben ser identificadas e implementadas teniendo en cuenta el tipo de riesgo, definiendo la probabilidad y el impacto del mismo.
- La seguridad debe estar presente durante el diseño de cualquier componente de TI y de cualquier arquitectura de TI.
- Las redes de computadores y sistemas externos son considerados como inseguros.

5.4 POLÍTICAS DE ACCESO

- La inclusión, actualización y eliminación de derechos de acceso, se realizará mediante peticiones formales, aprobación y controles previos.
- La eliminación de derechos se hará con un procedimiento que indique que el contrato se ha dado por terminado.
- Los perfiles de usuarios deben permitir o no la utilización de determinadas opciones o servicios.
- Cada proceso tendrá un responsable para su correcto funcionamiento.
- Las políticas de acceso serán revisadas por el comité de tecnología y puestos a disposición del directorio para su aprobación.
- El ingreso al centro de cómputo estará limitado con el uso de huellas dactilares y llaves del mismo.

- Los cambios que se necesiten realizar y que estén relacionados con el negocio, serán tramitados por el personal que se autorice para dicho efecto.
- Las claves que se utilicen para acceder a cualquier servicio del negocio, deben contener al menos: Dos o tres letras mayúsculas, dos o tres letras minúsculas, un número y un carácter especial.
- Las claves que se utilicen para acceder a cualquier servicio del negocio, debe estarán encriptadas y enmascaradas.
- Se identifican IDS (Sistema de detección de intrusos), IPS (Sistemas de prevención de intrusos), firewalls, entre otros, para controlar el acceso.
- No se podrá acceder a la instalación de software no autorizado, salvo con la respectiva autorización.
- La información concerniente al negocio podrá ser actualizada o modificada de acuerdo a la asignación de derecho que se haya realizado al personal encargado y se mantendrá un log de dichos cambios.
- Se monitoreará de forma periódica los accesos a operaciones catalogadas como privilegiadas o intentos de acceso no autorizados.
- Se controlará que los administradores no tengan acceso a borrar o desactivar pistas de sus propias actividades.
- Se deberá aplicar la política de escritorio limpio.
- El escritorio del computador solo puede contener el logo del negocio.
- El computador debe bloquearse inmediatamente después de un tiempo de no uso de 5 minutos.
- Debe guardarse una copia de todos los accesos de usuarios en un servidor que se designe para ello.

5.4.1 POLÍTICAS A NIVEL FÍSICO

- Todo el personal contará con su respectiva tarjeta de identificación. En estas tarjetas debe estar anotado la política de gestión integrada.
- El personal externo deberá recibir una tarjeta de visita. En estas tarjetas debe estar anotado la política de seguridad de la información y mecanismo para reportar incidentes de seguridad.
- Al ingresar o salir de la Oficina, todo el personal deberá registrar en el lector biométrico su ingreso o salida. En el evento de que un grupo de colaboradores llegue o salga de la Oficina, cada uno de ellos deberá registrar individualmente su ingreso o salida.
- Ninguna persona de la compañía podrá entregar su clave personal secreta, cada persona es responsable por dicha clave.
- Los empleados y funcionarios de la compañía utilizarán los programas o equipos conforme a los convenios de licencia, no se podrán utilizar programas sin licencia o copias de los mismos, así como tampoco se podrá utilizar música u otro tipo de programas obtenidos de Internet.
- Todos los programas o equipos que se necesiten para cumplir con sus labores deberán ser solicitados a los responsables de dicha área.
- Todo equipo que quiera ser conectado a la red de la compañía deberá contar con el respectivo permiso.
- Se prohíbe fumar o encender cigarros o botar colillas de cigarrillos en cualquier área que llegue a afectar equipos o programas de la compañía.
- Se prohíbe ingerir bebidas alcohólicas.
- Se debe mantener los respectivos equipos de control de fuego en caso de incendios.

5.4.2 POLÍTICAS A NIVEL LÓGICO

- Todos los equipos tienen bloqueo de puertos USB y la unidad de DVD y su reasignación se hará vía HelpDesk.
- Todos los equipos cuentan con software antivirus empresarial.
- Cada mes se solicitara el cambio de la contraseña de acceso al computador.
- La clave de acceso al correo electrónico será cambiada con el correspondiente permiso y solamente por el personal de Soporte Técnico.
- No se autoriza a abrir el case del equipo. Esta actividad está reservada solo al personal de Soporte Técnico.
- Las claves que se utilicen para acceder a cualquier servicio del negocio, deben contener al menos: Dos o tres letras mayúsculas, dos o tres letras minúsculas, un número y un carácter especial.
- Las claves que se utilicen para acceder a cualquier servicio del negocio, debe estar encriptadas y enmascaradas.
- Se identifican IDS (Sistema de detección de intrusos), IPS (Sistemas de prevención de intrusos), firewalls, entre otros, para controlar el acceso.
- El uso de WIFI para personas externas estará regulado por una política de asignación de contraseñas temporales y por cada sesión que se requiera.

5.4.3 POLÍTICAS DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN

- Las copias de respaldo de la información se realizaran dos veces en el día a intervalos definidos.

- Los respaldos se harán mediante la herramienta correspondiente y serán almacenados en una unidad de almacenamiento externo.
- Se deben realizar pruebas de restauración, al menos tres veces al año.

5.4.4 POLÍTICAS DE MANTENIMIENTO DE EQUIPOS

- Se debe establecer un inventario de equipos donde se identifique al responsable, su nivel de riesgo, su nivel de seguridad y mitigación.
- Aplicar una metodología de control de calidad y poner a prueba la infraestructura y los ajustes relacionados con la seguridad en entornos dedicados que termina con una prueba de aceptación formal.
- Recopilar, analizar y establecer un proceso de aprobación de las solicitudes de cambio.
- Definir procedimientos y responsabilidades
- Garantizar las medidas de seguridad adecuadas en el transporte de datos en medios físicos fuera de los locales del centro de datos.
- Garantizar los principios de seguridad que se aplican en la arquitectura de red y sus componentes, estableciendo las diferentes zonas de seguridad separadas por sus correspondientes puertas de enlace y la clasificación de la información.
- Aprobar los cambios de configuración y la revisión de logs del FIREWALL.
- Identificar los recursos críticos de servicios de TI.
- Se debe garantizar el monitoreo y planificación en la revisión de capacidades del equipo.

5.4.5 POLÍTICAS DE USO DE SOFTWARE

- Los usuarios no deben instalar o intentar instalar programas, utilitarios o complementos para navegadores de internet. Esta actividad está reservada solo al personal de Soporte Técnico de la empresa.
- Está prohibido el uso de programas sin licencias no autorizadas por la empresa.
- Todo equipo de computación debe mantener en forma residente un antivirus instalado y las actualizaciones de las nuevas versiones, deben realizarse en línea.

5.4.6 POLÍTICAS DE INFORMACIÓN DE LOS SISTEMAS

- Se debe mantener un inventario de la información así como de las aplicaciones señalando a su correspondiente responsable.
- Se debe definir un esquema de información clasificada y aplicaciones especificando el nivel de riesgo, su nivel de seguridad y su mitigación.
- Deben existir requerimientos para realizar cualquier cambio a o los sistemas con los que consta la compañía.
- Se deben aplicar las pruebas necesarias antes de realizar la actualización del software.
- Debe existir un plan de actividades post implementación que permita detectar posibles fallas.
- Debe existir un procedimiento para aplicar cambios en casos de emergencia.

CAPÍTULO 6

IMPLEMENTACIÓN

6.1 DEFINICIÓN DE CASOS

A continuación se describen dos casos que están relacionados de forma directa con el proceso de emisión de pólizas. El primero trata sobre la emisión de pólizas referidas y el segundo se vincula con el proceso de cotizaciones en general y como se ve afectado por cambio no controlado de hardware. A modo referencial se indicará que las pólizas referidas son aquellas cuyos términos y condiciones son fijados directamente por un reasegurador a nivel internacional para un cliente o asegurado que de igual forma tiene presencia internacional en lo que a sus negocios se refiere. Este contrato de seguro está respaldado por la Compañía de Seguros a nivel local quien acepta la representación de dicho reasegurador para un determinado asegurado, ganando por esa representación un porcentaje de comisión establecido de antemano.

6.2 EMISIÓN DE PÓLIZA REFERIDA

Se entiende como pólizas referidas aquellas cuyos términos y condiciones son fijados directamente por un reasegurador a nivel internacional para un cliente o asegurado que de igual forma tiene presencia internacional en cuanto a sus negocios se refiere. Este contrato de seguro está respaldado por la Compañía de Seguros a nivel local quien acepta la representación de dicho reasegurador para un determinado asegurado, ganando por esa representación un porcentaje de comisión establecido de antemano.

Este tipo de pólizas a pesar de ser internacionales cumplen con el ciclo de vida del proceso de emisión de pólizas mostrado anteriormente, mismo que va desde la cotización, pasando por el posicionamiento del reaseguro hasta la emisión de la póliza y su correspondiente facturación. En este tipo de negociaciones se obvia la participación del Departamento Comercial al momento de cotizar la póliza ya que por ser una póliza de carácter especial y con características distintas a las que normalmente se emiten, pasan a ser manejadas por el Área Técnica en conjunto con el Área de Operaciones, quienes se responsabilizan por la cotización, establecimiento de valores asegurados, verificación de coberturas y límites del riesgo y la emisión de la documentación requerida por el cliente.

6.2.1 DESCRIPCIÓN DEL CASO

El cliente EVEREADY quien tiene representación en varios países del mundo, se acerca a la compañía aseguradora para realizar la petición del seguro. El primer acercamiento lo realiza directamente con la Gerencia General quien a su vez lo deriva con el Gerente Técnico y con el Gerente

de Operaciones para dar comienzo con las negociaciones. El proceso se detalla a continuación:

a) El Gerente Técnico procede con la revisión de las condiciones y términos fijados por el reasegurador del exterior.
b) El Gerente Técnico comienza con la extracción a partir de la documentación entregada, de: Coberturas, Cláusulas y Deducibles y es aquí donde comienza el primer problema, ya que las coberturas y cláusulas del reasegurador del exterior por ser más amplias no se acoplan totalmente con las que la compañía otorga, debiendo el Área Técnica buscar las más parecidas a las que ofrece dicho reasegurador. Una vez realizada la evaluación y análisis de la información, el Área Técnica entrega toda la documentación al Área de Operaciones representada por su Gerente de Operaciones.
c) El Gerente de Operaciones recibe la documentación con el visto bueno del Gerente Técnico y procede a entregar toda la información a un ejecutivo de su departamento para de esta forma comenzar con su trabajo que ya no es analizar la información recibida sino ingresar dicha información en el Sistema Informático y es aquí donde aparece el segundo problema. El ejecutivo de Operaciones al tratar de ingresar la póliza se encuentra con que existen cláusulas y coberturas definidas en la documentación que no aparecen en el Sistema Informático, por lo que creyendo que es un error procede a regresar los papeles al Área Técnica.
d) El tercer problema aparece cuando tanto el Gerente Técnico como el Gerente de Operaciones no logran ponerse de acuerdo en relación con los términos y condiciones del contrato de seguro y es entonces

cuando el Gerente de Operaciones entrega nuevamente los papeles al ejecutivo de operaciones y le encomienda ingresar la póliza obviando el procedimiento de escoger las coberturas y cláusulas definidas en el sistema y procediendo a ingresar toda la información tal cual fue recibida por el Área Técnica. Esto trae consigo errores de ingreso y de estructura por falta de información en referencia al tema.

e) Una vez terminada la póliza, esta es devuelta al Área Técnica representada por su Gerente Técnico quien demuestra su inconformidad por recibir un documento sin la estructura general de las otras pólizas que no son referidas, más obvia esa parte y concentra su atención en la revisión de que todas las cláusulas y coberturas ingresadas se encuentren conforme con lo entregado por el reasegurador internacional.

f) En el intermedio de las revisiones, correcciones y emisión de la póliza, tanto el Gerente Técnico como el Gerente de Operaciones deben salir de la oficina para concretar otra negociación, olvidando que para ese mismo día el cliente referido necesitaba su póliza. Siendo en este punto el ejecutivo del Área de Operaciones, quien se queda con la responsabilidad de la culminación de dicha póliza así como su entrega inmediata debido a la premura del cliente por recibir su documentación.

g) En el camino, el ejecutivo de Operaciones se encuentra con algunas dudas en referencia a las correcciones pedidas por el Área Técnica, al no encontrarse el Gerente Técnico ni tampoco el Gerente de Operaciones, decide ingresar ciertos parámetros de acuerdo a su propio análisis, experiencia e intuición y con ello dar por terminada la

emisión de la póliza, todo esto porque ya tiene como agravante la urgencia del cliente por recibir su contrato de seguro.

6.2.2 ROLES QUE INTERVIENEN EN EL CASO

Los roles presentes en este caso son: Gerente de Operaciones, Gerente Técnico y Ejecutivo de Operaciones, de entre sus responsabilidades tenemos:

Ejecutivo de Operaciones

- ✓ Revisión de solicitudes de emisión y análisis en base a políticas de suscripción
- ✓ Llevar un control y seguimiento a los folios asignados por el Gerente de Operaciones por trámite u orden de trabajo.
- ✓ Administrar el proceso de emisión y armado para garantizar el cumplimiento en tiempos de emisión y estándares de servicio establecidos por convenio
- ✓ Cumplir con las políticas de seguridad de la empresa.

Gerente de Operaciones

- ✓ Trabajar en conjunto con la Gerencia General en el plan estratégico de la Compañía de Seguros.
- ✓ Proponer políticas y procedimientos para la Gestión Integral de Riesgos.
- ✓ Desarrollo de controles apropiados para dar soporte a la continuidad del negocio.

- ✓ Monitorear el cumplimiento de las políticas y delineamientos establecidos para la continuidad del negocio.
- ✓ Promover cultura organizacional de riesgos.
- ✓ Supervisar y controlar la ejecución de las políticas, normas y procedimientos establecidos para la suscripción de los ramos que maneja la empresa.

Gerente Técnico

- ✓ Trabajar en conjunto con la Gerencia General en el plan estratégico de la Compañía de Seguros.
- ✓ Proponer políticas y procedimientos para la Gestión Integral de Riesgos.
- ✓ Controlar las operaciones técnicas y operativas.
- ✓ Optimizar procesos de gestión en áreas operativas.
- ✓ Coordinar las actividades del proceso técnico de Cotización y Suscripción de la póliza.
- ✓ Asesorar y atender la renovación de pólizas de clientes importantes.
- ✓ Colaborar con el área de Operaciones para dar cumplimiento a lo dispuesto por la empresa.

6.2.3 POLÍTICAS LIGADAS AL ROL

Las políticas que se aplican son:

Ejecutivo de Operaciones

- ✓ Garantizar que la póliza no tenga errores de definición o estructural.

- ✓ Presentar al cliente de forma clara y precisa las coberturas, cláusulas y condiciones, así como también valores en referencia a: primas, impuestos y deducibles relacionados con el contrato del seguros.

Gerente de Operaciones

- ✓ Asignar personal con el suficiente conocimiento técnico tanto para la cotización del seguro como para la emisión del mismo.
- ✓ .Garantizar que los valores cobrados a nivel de prima e impuestos sean correctos y respalden la eventualidad de ocurrencia de un siniestro.
- ✓ Redactar la póliza de forma clara para el asegurado.

Gerente Técnico

- ✓ Debe haber una separación real de autoridad y responsabilidad para asegurar que ningún individuo tiene control exclusivo de una pieza de información
- ✓ Recabar información suficiente en referencia al riesgo que se desea aceptar.
- ✓ Ceñir el contenido de la póliza de acuerdo a lo dispuesto en la legislación sobre el contrato de seguro constante en el Código de Comercio, el decreto supremo No. 1147 publicado en el Registro Oficial No. 123 de 7 de diciembre de 1963, a la presente Ley y a las demás disposiciones que fueren aplicables.

6.2.4 CONTROLES APLICADOS

Por lo que al activarse las siguientes amenazas se mitigan con los controles descritos anteriormente:

Tabla 15 Caso No. 1 Amenazas, Vulnerabilidades y Controles

AMENAZA	VULNERABILIDAD	CONTROLES
[E.7] Deficiencias en la organización	• E.7.1 Acciones no coordinadas • E.7.2 Errores por omisión • E.7.3 Roles mal definidos • E.7.4 Desconocimiento de procedimientos	• A.18.2.2 Cumplimiento en las políticas y normas de seguridad • A.17.1.1 Planificación de la continuidad de la seguridad de la información • A.18.1.3 Protección de registros • A.14.2.7 Desarrollo contratado externamente • A.14.2.8 Pruebas de seguridad de sistemas
[A.7] Uso no previsto	• A.7.1 Ausencia de procedimientos de manejo de información clasificada • A.7.3 Documentación con fallas estructurales no acordes a la organización	
[E.21] Errores de mantenimiento y actualización de programas	• E.21.2 Procedimientos y controles ineficientes para revisiones de software contratado externamente. • E.21.3 No cumple con reglas del negocio	

6.3 BLOQUEO EN ENVÍO DE COTIZACIONES

Teniendo como antecedente la mala situación del país y con ello la necesidad de captar nuevos clientes y/o mantener la cartera que se considera renovable, la compañía de seguros tiene como política la generación diaria de cotizaciones para clientes que ya tuvieron una póliza en el período pasado y que están próximos a vencerse o de clientes que han demostrado su intención por adquirir un determinado seguro.

Esta actividad es realizada por el Departamento Comercial quienes para cumplir con este objetivo tienen un horario de entrada adelantado, motivo por el cual

necesitan contar con toda la infraestructura a nivel de Hardware, Software y Comunicaciones que les permita realizar dichas labores.

6.3.1 DESCRIPCIÓN DEL CASO

a) El Gerente Comercial revisa su buzón de correo para verificar los informes recibidos por el Área de Renovaciones y/o Suscripciones, con lo cual procede a dividir el trabajo para cada uno de sus ejecutivos.

b) Los ejecutivos del área Comercial dan aviso a su Gerente Comercial que no reciben el correo donde consta la lista de los clientes a los cuales deben generar una cotización.

c) El Gerente Comercial opta entonces por entregarles a cada uno de sus ejecutivos la impresión de los informes tanto de clientes que se van a renovar como de los clientes nuevos para que procedan con la generación de la cotización.

d) Los ejecutivos del área Comercial intentan ingresar al sistema para proceder con la cotización de los clientes, más notan que no lo pueden hacer, cuestión que nuevamente es comunicada a su Gerente Comercial.

e) El Gerente Comercial ante estos dos problemas realiza una llamada al Área de TI para que revisen lo reportado por cada uno de sus ejecutivos.

f) En el Área de TI la llamada es recibida por uno de los asistentes del departamento, quien a su vez intenta dar aviso al Administrador del Centro de Cómputo sin encontrarlo disponible.

g) Luego de treinta minutos se logra comunicación con el Administrador del Centro de Cómputo quien comienza a realizar las revisiones del

Servidor tanto de correos como del Servidor de Producción donde reside el Sistema Integrado de Seguros.

h) Ha pasado una hora ya desde que se reportó el incidente y no se encuentra solución para ninguno de los dos problemas, por lo que el Administrador del Centro de Cómputo procede a dar de baja ambos servidores.

i) Como antecedente es preciso indicar que la noche anterior el Administrador del Centro de Cómputo, estuvo haciendo labores de instalación de un nuevo FIREWALL con un proveedor externo, por lo que se hicieron modificaciones y adecuaciones a dicho equipo.

j) Al restablecer los servidores (producción y correos) el Administrador de Base de datos nota que la comunicación a nivel del servidor de correos no se soluciona, pero encuentra que el problema del Servidor de producción se produjo por falta de espacio en el mismo, por lo que procede con la eliminación de archivos temporales y de archivos de trabajo no necesarios.

k) Ya casi al mediodía el Administrador de Centro de Cómputo encuentra que el problema por el cual no se tiene el servicio de correos es por una mala configuración realizada por los proveedores externos en relación al nuevo FIREWALL instalado.

l) Vía telefónica se mantiene comunicación con dichos proveedores ya que indican que el soporte ante eventuales problemas solo se da a través de personal que reside en el exterior, cuestión que no habían informado con anterioridad.

m) Aproximadamente a las cuatro de la tarde se logra restablecer el servicio de correos y se da aviso a los usuarios para que procedan

con sus labores, manteniéndose aún otros problemas relacionados con el cambio de FIREWALL.

6.3.2 ROLES QUE INTERVIENEN EN EL CASO

Los roles presentes en este caso son: Gerente Comercial, Ejecutivo Comercial y Jefe de TI, de entre sus responsabilidades tenemos:

Gerente Comercial

- ✓ Alinear su estrategia con la política dictada por el directorio y busca la mejor manera de alcanzar los objetivos y metas planteados.
- ✓ Supervisar el trabajo del equipo.
- ✓ Definir y dirigir la estrategia comercial.
- ✓ Analizar y desarrollar productos y servicios
- ✓ Coordinar la renovación de clientes

Ejecutivo Comercial

- ✓ Coordinar con la gerencia Comercial la ejecución de metas y objetivos.
- ✓ Atender los requerimientos y solicitudes de seguros de los clientes
- ✓ Gestionar las cotizaciones para su presentación y aprobación por el cliente.
- ✓ Controlar el Vencimiento de Pólizas, mediante mails, cartas o comunicados.
- ✓ Presentar a la Gerencia Comercial un reporte mensual de las pólizas por vencer a fin de determinar las estrategias más convenientes para cierre de las renovaciones

Jefe de TI

- ✓ Planear, organizar, Dirigir y Controlar, el funcionamiento del Área de Sistemas.
- ✓ Coordinar la atención y resolución de problemas y requerimientos
- ✓ Evaluar e identificar los riesgos informáticos que pueden llegar a amenazar la continuidad del negocio.
- ✓ Trabajar en conjunto con la Gerencia General para clarificar los riesgos del negocio y diseñar planes de acción.
- ✓ Garantizar la disponibilidad de los sistemas.
- ✓ Implementar procedimientos para la recuperación del sistema en caso de fallos.
- ✓ Diseñar en conjunto con la Gerencia General el DRP de acuerdo a los riesgos que se encuentra expuesto el negocio.
- ✓ Alinear la estrategia de tecnologías de la información con las del negocio.

6.3.3 POLÍTICAS LIGADAS AL ROL

Las políticas que se aplican son:

Gerente Comercial

- ✓ Garantizar la entrega de cotizaciones al cliente y/o bróker de negocios a renovarse considerando como mínimo un mes de anticipación.
- ✓ Garantizar que las cotizaciones a procesarse pertenezcan a clientes que han sido objeto de estudio, tanto a nivel de sus siniestros, como de su cartera y datos requeridos para la Unidad de Lavado de Activos.

Ejecutivo Comercial

- ✓ Cumplir con llenado de documento de conozca a su cliente
- ✓ Informar al cliente sobre el valor del seguro de acuerdo a la inspección realizada
- ✓ Garantizar que los valores cobrados a nivel de prima e impuestos sean correctos y respalden la eventualidad de ocurrencia de un siniestro.

Jefe de TI

- ✓ La información de los sistemas deberá estar siempre disponible para asuntos del negocio.
- ✓ Aplicar una metodología de control de calidad y poner a prueba la infraestructura y los ajustes relacionados con la seguridad en entornos dedicados que termina con una prueba de aceptación formal.
- ✓ Garantizar los principios de seguridad que se aplican en la arquitectura de red y sus componentes, estableciendo las diferentes zonas de seguridad separadas por sus correspondientes puertas de enlace y la clasificación de la información
- ✓ Aprobar los cambios de configuración y la revisión de LOGS del FIREWALL.
- ✓ Identificar los recursos críticos de servicios de TI.
- ✓ Garantizar el monitoreo y planificación en la revisión de capacidades del equipo.

6.3.4 CONTROLES APLICADOS

Por lo que al activarse las siguientes amenazas se mitigan con los controles descritos anteriormente:

Tabla 16 Caso No. 2 Amenazas, Vulnerabilidades y Controles

AMENAZA	VULNERABILIDAD	CONTROLES
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	E.23.1 Desconocimiento de procedimientos o controles de actualización de equipos.	• A.11.2.4 Mantenimiento de equipos • A.8.1.2 Propiedad de los activos • A.8.1.3 Uso aceptable de equipos • A.11.2.8 Equipos de usuario desatendido • A.12.3.1 Respaldo de información • A.18.2.2 Cumplimiento en las políticas y normas de seguridad • A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información • A.13.2.3 Mensajería electrónica • A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos de los proveedores • A.18.2.3 Revisión del cumplimiento técnico • A.9.1.1 Política de control de acceso • A.18.2.2 Cumplimiento en las políticas y normas de seguridad • A.12.4.1 Registro de eventos
[E.2] Errores del administrador	• E.2.1 Desconocimiento en instalación de equipos	
[I.5] Avería de origen físico o lógico	• I.5.1 Fallos en los equipos por defecto de origen	
[A.23] Manipulación de los equipos	• A.23.2 Mala administración en mantenimiento de equipos • A.23.2 Overflow por falta de verificación de capacidades del equipo	
[E.7] Deficiencias en la organización	• E.7.1 Acciones no coordinadas • E.7.2 Errores por omisión • E.7.4 Desconocimiento de procedimientos	
[E.24] Servicio inhabilitado	• E.24.4 Errores de configuración • E.24.5 Tareas programadas con protección inadecuada. • E.24.6 Enlace de internet caído.	
[A.7] Uso no previsto	• A.7.2 Errores del administrador • A.7.3 Desconocimiento de políticas de uso del servicio	
[A.4] Manipulación de la configuración	• A.4.1 Inexperiencia en administración de configuración.	

CAPÍTULO 7

ANÁLISIS DE RESULTADOS

7.1 ANÁLISIS DE RESULTADOS DE ACUERDO A CONTROLES IMPLEMENTADOS

Para tener una idea más clara en cuanto a los casos presentados, se llevó a cabo un cuestionario de tal forma que sea factible tener una visión descriptiva y con ello detectar aspectos positivos y negativos en torno al desenvolvimiento de la empresa de seguros en cuanto a los objetivos y labor que cada miembro debe desarrollar. Cuestión que se indicará para cada uno de los casos expuestos.

7.1.1 EMISIÓN DE PÓLIZA REFERIDA

La principal amenaza que se logró detectar fue la deficiencia en la organización en cuanto a desconocimiento de procedimientos, acciones no coordinadas y dudas en cómo realizar el trabajo asignado. De acuerdo a la encuesta realizada a un total de diez personas pertenecientes al área de operaciones se pudo extraer lo siguiente:

Tabla 17 Cuestionario realizado al área de operaciones

¿Cuánto tiempo llevas trabajando en la empresa?

	Cantidad	Porcentaje
a) De 1 a 6 meses	0	0.00%
b) De 6 meses a 1 año	2	20.00%
c) De 1 año a 3 años	3	30.00%
d) Más de 3 años	5	50.00%
Total	10	100.00%

¿Quién te enseñó a realizar tu trabajo?

	Cantidad	Porcentaje
a) Un compañero	4	40.00%
b) Tu Jefe	0	0.00%
c) Leí manual	1	10.00%
d) Aprendí con experiencia	3	30.00%
e) Sistemas	2	20.00%
Total	10	100.00%

¿Cuánto tiempo te llevó conocer tu trabajo?

	Cantidad	Porcentaje
a) Un día	0	0.00%
b) Una semana	0	0.00%
c) De 1 mes a 3 meses	1	10.00%
d) De 3 meses a 6 meses	8	80.00%
e) Más de 6 meses	1	10.00%
Total	10	100.00%

¿En el momento que te contrataron sabias exactamente qué hacer?

	Cantidad	Porcentaje
a) SI	6	60.00%
b) NO	4	40.00%
Total	10	100.00%

¿Quién te indicó cuales serían tus responsabilidades?

	Cantidad	Porcentaje

a) Un compañero	0	0.00%
b) Tu Jefe	2	20.00%
c) Recursos Humanos	8	80.00%
d) Nadie	0	0.00%
Total	10	100.00%

Cuando realizas tu trabajo ¿Tienes dudas de cómo hacerlo?

	Cantidad	Porcentaje
a) SI	2	20.00%
b) NO	0	0.00%
c) A VECES	8	80.00%
Total	10	100.00%

Cuando tienes dudas ¿Quién te las aclara?

	Cantidad	Porcentaje
a) Un compañero	3	30.00%
b) Tu Jefe	3	30.00%
c) Sistemas	4	40.00%
d) Nadie	0	0.00%
Total	10	100.00%

¿En algún momento sentiste que no sabías lo suficiente para realizar el trabajo?

	Cantidad	Porcentaje
a) SI	10	100.00%
b) NO	0	0.00%
Total	10	100.00%

¿Se mide el desempeño de tu puesto?

	Cantidad	Porcentaje
a) SI	0	0.00%
b) NO	10	100.00%
Total	10	100.00%

Con estos resultados se establece:

a) No existe una correcta inducción en referencia al puesto de trabajo que se asigna, donde se incluya funciones y métodos que correspondan a la función que se vaya a realizar y en donde de ser factible se integre con la mayor cantidad de personal involucrado.
b) No se establece una agenda para cada actividad que se asigna.
c) No se explica de modo general las normas y políticas establecidas en la empresa.
d) No se explican los objetivos básicos en relación a la seguridad de la información.
e) No existe una concientización en referencia a las amenazas y ataques a los que se puede estar expuesto en lo que se refiere a la seguridad de la información.
f) No existe un plan de continuidad del negocio actualizado
g) No existe una gestión de riesgos continua.
h) No existen procedimientos actualizados acorde con el crecimiento que ha tenido la empresa a lo largo del tiempo.
i) No existe una medición de las actividades claves del negocio de tal forma que se pueda determinar su eficacia y eficiencia.
j) No existe conciencia de la estrategia que la organización va a implementar.

7.1.2 BLOQUEO EN ENVÍO DE COTIZACIONES

En este proceso se encontraron las siguientes amenazas:

a) Mala administración de la actualización de equipos
b) Mantenimiento inadecuado

c) Mala manipulación de configuración
d) Caída del sistema por servicio no disponible

En relación a estos puntos se evidencia:

a) No existen estándares y procedimientos para el cambio de equipos.
b) No existen guías que sirvan de base en la implementación de un determinado equipo.
c) Administración deficiente del centro de cómputo.
d) No se aplica de forma estricta las normas de seguridad y control establecidas.
e) No existe planificación en la modificación e instalación de nuevo hardware.
f) Deficiente coordinación con los técnicos del proveedor a fin de garantizar la instalación de los equipos.

7.2 EVALUACIÓN DE EFICIENCIA ACORDE CON ACCIONES TOMADAS

En relación a los casos presentados se detalla a continuación las indicaciones necesarias para cada procedimiento.

Emisión de póliza referida

a) Realizar el entrenamiento constante a los colaboradores para atender mejor al cliente, lo cual es primordial dentro del ámbito del negocio ya que se podrá tener personal más capacitado que pueda tomar las decisiones correctas en el momento indicado.

b) Realizar la revisión de los procedimientos y procesos que se requieren para la emisión de pólizas referidas.
c) Realizar campaña de concientización en referencia a las responsabilidades que tiene cada individuo en relación a la seguridad de la información.
d) Dar a conocer la política de seguridad con el fin de que cada persona conozca la importancia de proteger la información.
e) Realizar la revisión de procesos en conjunto con el personal involucrado con la finalidad de hallar posibles fallas en dichos procesos.
f) Realizar cronograma de actividades que permita organizar el tiempo que se utiliza para la emisión de pólizas referidas.
g) Guiar la emisión de pólizas referidas en base a lo dispuesto en la legislación sobre el contrato de seguro constante en el Código de Comercio, el decreto supremo No. 1147 publicado en el Registro Oficial No. 123 de 7 de diciembre de 1963, a la presente Ley y a las demás disposiciones que fueren aplicables.
h) Guiar la emisión de pólizas referidas de acuerdo a lo expuesto en los libros I y II, títulos X, V, VI, XII, capítulos I, II, IV de la ley de seguros, así como las resoluciones JB-011-2014-F y JB-2014-3066 entregadas por la superintendencia de compañías.
i) Mejorar los procesos de comunicación.

Bloqueo en envío de cotizaciones

a) Analizar concienzudamente los cambios que se realizaran, tomando en consideración las características, configuraciones y estructuras de control.
b) Identificar los requisitos de seguridad de la empresa.
c) Establecer y documentar las pautas necesarias para la implementación de equipos.

d) Establecer umbrales efectivos para protegerse de ataques mediante la utilización de estadísticas de tráfico.
e) Tener un plan de trabajo para el mantenimiento de equipos.
f) Mantener el sistema disponible para los usuarios.
g) Revisar resultado de implementación de equipos e introducir acciones que permitan corregir las falencias encontradas.
h) Llevar registro de fallas, problemas y soluciones concerniente a la instalación de nuevos equipos.

CONCLUSIONES Y RECOMENDACIONES

1. La protección de la información y de los activos de los que dispone la empresa dependen de una correcta gestión de seguridad de información, lo cual asegura la continuidad del negocio y minimiza el impacto de incidentes que puedan llegar a ocurrir.
2. La Confidencialidad, Integridad y Disponibilidad son componentes fundamentales de la gestión de seguridad de información y le permiten a la empresa garantizar y asegurar que tanto los sistemas de información como los activos de información tengan un nivel de protección idóneo a la hora de enfrentar alguna amenaza.
3. Es necesario concienciar a los empleados de la empresa ya que todas las decisiones que se toman a diario pueden llegar a afectar la seguridad de la información, por lo cual se los debe educar para que puedan identificar y responder ante posibles incidentes.
4. Es importante identificar las necesidades de seguridad y los riesgos informáticos a los que se encuentra expuesto el negocio con la finalidad de estar en la capacidad de controlar y detectar vulnerabilidades y contrarrestar las falencias en las aplicaciones y los equipos que se utilizan.

5. La Gerencia debe estar involucrada tanto en el análisis, desarrollo e implementación de reglas, procedimientos, estrategias y mecanismos de seguridad tanto físicos como lógicos así como en un plan de recuperación en caso de llegar a ocurrir un incidente de seguridad.
6. La empresa debe conocer el tipo de activo de información que posee, quienes están autorizados o son responsables de ellos y su valoración para identificar su impacto en la organización.
7. Magerit en su libro dos, catálogo de elementos, provee una agrupación de amenazas en cuatro grandes grupos, así como la información para dimensionar las amenazas a las que se hayan expuestos los activos, sean estos de información, físicos, de TI o humanos.
8. Los sistemas de Gestión de Seguridad de Información bajo la norma ISO 27001, se basan en la prevención, por lo tanto es muy importante identificar los riesgos a los que están expuestos los activos para así evitar pérdidas económicas u operacionales.
9. La gerencia debe revisar y definir de manera constante los controles, amenazas y vulnerabilidades presentes e iniciar acciones correctivas y preventivas a cada momento.
10. Una vez identificados los riesgos a los que están expuestos los activos de información, es necesario implementar controles o salvaguardas, con la finalidad de proteger estos activos y lograr minimizar la probabilidad de que se materialicen los riesgos o el impacto que pueden tener sobre la organización.
11. El estándar ISO 27001-2013 es un sistema de gestión de seguridad de información, cuyo propósito es mitigar los riesgos a partir del análisis y evaluación de los activos de información mediante el establecimiento de controles que tienen gran aceptación en los mercados internacionales.

RECOMENDACIONES

1. Establecer esquemas eficientes de control y administración de los riesgos que permitan medir, controlar y monitorear las exposiciones del riesgo en referencia al desarrollo normal del negocio.
2. Actualizar permanentemente las estrategias, políticas y procedimientos para una eficiente administración del riesgo.
3. Crear cultura de seguridad concientizando, divulgando y formando al personal de la compañía en relación a las actividades que se están llevando a cabo para mejorar la transparencia de los procesos e involucrándolos en el establecimiento de objetivos sólidos en lo que se refiere al tema de seguridad de la información.
4. Establecer una estructura organizativa que defina de forma clara los procesos, responsabilidades e interrelación entre las diferentes áreas de la compañía de seguros.
5. Especificar responsabilidades acorde con las características y complejidad de cada riesgo enfocado en la suscripción del contrato de seguros, tales como: Riesgo de crédito, riesgo operacional, riesgo de liquidez, etc.
6. Asegurar que la compañía de seguros cuente con el personal, material y equipo adecuado para reducir o minimizar el riesgo.

7. Disponer de un sistema informático que provea la información necesaria para medir, controlar y monitorear las exposiciones de riesgo y apoyar en la toma de decisiones oportunas y adecuadas.
8. Establecer un reporte de incidentes que permita estar al corriente de los eventos ocurridos por debilidades en la seguridad de la información de tal forma que pueda ser comunicado y con ello se puedan tomar acciones correctivas.

BIBLIOGRAFÍA

[1] Organización Internacional para la Estandarización (ISO). http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm

[2] Portal ISO 27001 España, Norma ISO27001. http://www.iso27000.es/iso27000.html

[3] Alberto G. Alexander. Diseño de un Sistema de Gestión de Seguridad de Información- Óptica ISO 27001:2005, Alfa omega ,http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf, 2007

[4] Ministerio de Hacienda y Administraciones Públicas – Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.

[5] Ministerio de Hacienda y Administraciones Públicas – Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2 – Catálogo de elementos.

[6] ISOTools Organization, ISO 27001. El inventario de activos en la implementación de la norma**,** https://www.isotools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/, Diciembre-2013.

[7] Portal de Aplicación tributaria y manejo de información como activo, Argentina, Silvio R. de Cicco, La información es el activo más importante **http://www.aplimatica.com.ar/La-informacion-el-activo-mas-importante.html,** Septiembre-2014.

[8] El gerente de TI y su rol en la gestión inteligente de riesgos, José Antonio Lagos, Socio de Risk de Deloitte, http://www.emb.cl/gerencia/articulo.mvc?xid=1663, Agosto-2012.

[9] Superintendencia de Compañías del Ecuador, Normas generales para las instituciones del sistema financiero, Libro I, Título X, capítulo I,

http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_I.pdf ,Enero-2016.

[10] Superintendencia de Compañías del Ecuador , Normas generales para las instituciones del sistema financiero, Libro I, Título X, capítulo II, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_II.pdf,Enero-2016.

[11] Superintendencia de Compañías del Ecuador, Normas generales para las instituciones del sistema financiero, Libro I, Título X, capítulo III, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_III.pdf,Enero-2016.

[12] Superintendencia de Compañías del Ecuador, Normas generales para las instituciones del sistema financiero, Libro I, Título X, capítulo V, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf,Enero-2016.

[13] Revista ITNOW, Como hacer un plan de comunicación de seguridad, https://revistaitnow.com/como-crear-un-eficaz-plan-de-comunicacion-de-seguridad-de-datos/, Febrero-2015.

[14] Cabinet Office, in partnership with the Business Continuity Institute and Emergency Planning Society Government United Kingdom, https://www.gov.uk/government/news/business-continuity-guide-launched, Semtiembre-2012.

[15] Superintendencia de Compañías del Ecuador, Normas generales para las instituciones del sistema de seguro privado, Libro II, Título VII, capítulo I, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L2_VII_cap_I.pdf,Enero-2016.

[16] Superintendencia de Compañías del Ecuador, Normas generales para las instituciones del sistema de seguro privado, Libro II, Título VII, capítulo II,

http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L2_VII_cap_II.pdf,Enero-2016.

[17] Superintendencia de Compañías del Ecuador, Normas generales para las instituciones del sistema de seguro privado, Libro II, Título VII, capítulo III, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L2_VII_cap_III.pdf,Enero-2016.

[18] Superintendencia de Compañías del Ecuador, Normas generales para las instituciones del sistema de seguro privado, Libro II, Título V, capítulo I, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L2_V_cap_I.pdf,Enero-2016.

[19] Superintendencia de Compañías del Ecuador, Normas generales para las instituciones del sistema de seguro privado, Libro II, Título VI, capítulo I, http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L2_VI_cap_I.pdf,Enero-2016.

[20] Paúl Kivan Search Data Center, Guía de evaluación de riesgos de TI, http://searchdatacenter.techtarget.com/es/tutoriales/Guia-de-evaluacion-de-riesgos-de-TI#Primerospasosdeunaevaluacinderiesgo, Nov-2013.

[21] Instituto Nacional de Ciberseguridad de España, Implantación de un SGSI en la empresa, https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf , Nov-2012.

[22] Isabel Casares San José-Marti, España, Procesos de gestión de riesgos y seguros de las empresas, http://fundacioninade.org/sites/inade.org/files/primer_libro_isabel_casares.pdf , Nov-2013.

[23] Claudio Fernández, Unidad de Servicio de Seguros EVERIS, México, Estudio de Gestión de Riesgos en el Sector Asegurador,

http://www.everis.com/mexico/WCRepositoryFiles/GESTION%20RIESGOS%20EN%20EL%20SECTOR%20ASEGURADOR.pdf , Nov-2009.