DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: "GESTIÓN DE RIESGOS INFORMÁTICOS EN LA EMPRESA

FIDEVAL UTILIZANDO ISO 27001"

AUTOR: VILATUÑA CARDENAS, SANTIAGO FERNANDO

DIRECTOR: ING. DE LA TORRE, ARTURO

CODIRECTOR: ING. PÁLIZ, VÍCTOR

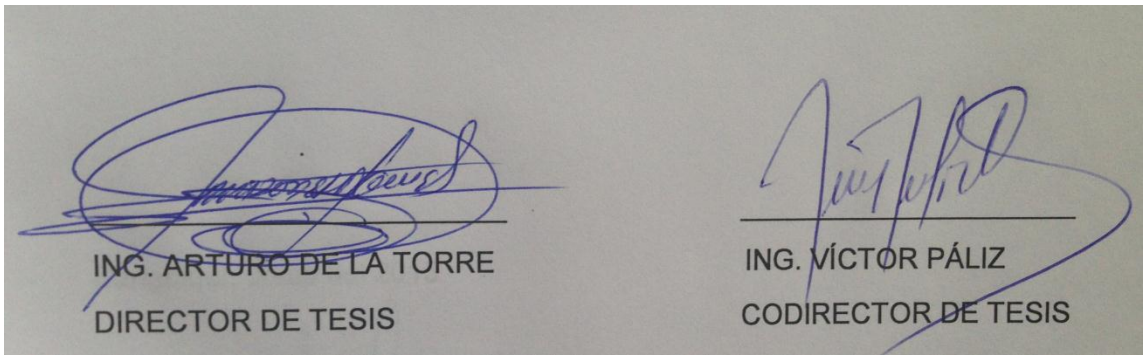
SANGOLQUÍ

2015

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. SANTIAGO FERNANDO VILATUÑA CÁRDENAS como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA.

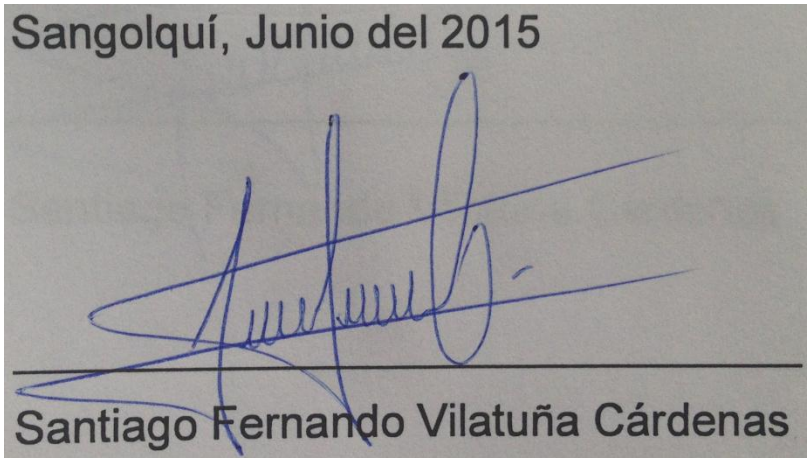
Sangolquí, Junio del 2015



AUTORÍA DE RESPONSABILIDAD

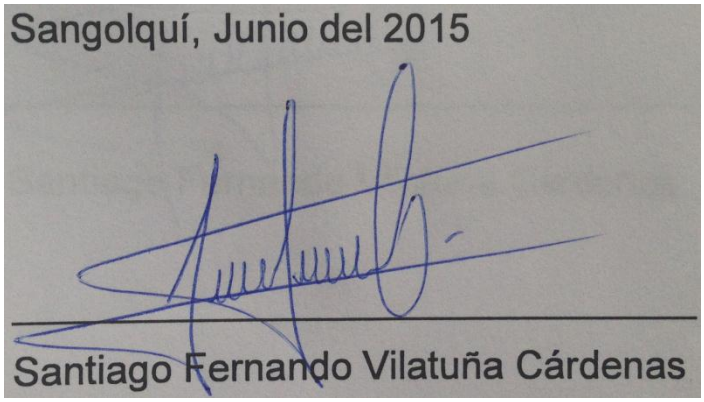
Yo, Santiago Fernando Vilatuña Cárdenas declaro que el presente trabajo es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación personal y que he consultado las referencias bibliográficas que se incluyen en el documento.

La Universidad de las Fuerzas Armadas ESPE puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual por su reglamento y por la normativa institucional vigente



AUTORIZACIÓN

Yo, SANTIAGO FERNANDO VILATUÑA CÁRDENAS, autorizo a la Universidad de las Fuerzas Armadas ESPE la publicación en el repositorio digital de la biblioteca Alejandro Segovia el presente proyecto denominado “GESTIÓN DE RIESGOS INFORMÁTICOS EN LA EMPRESA FIDEVAL UTILIZANDO ISO 27001”, así como también los materiales y documentos relacionados a la misma.



DEDICATORIA

A mi madre que es una persona especial en mi vida y que gracias a los valores que me inculco, a su cariño, al amor y a sus palabras de aliento para seguir siempre adelante he logrado llegar a la conclusión de este objetivo.

A mi padre que desde el cielo estará orgulloso de este logro, ya que siempre lucho por verme como una persona de bien, con sus sabios consejos y ejemplos.

A mi esposa Tannya a la cual amo y respeto, es una persona que admiro en demasía por su inmensa tenacidad, amor y cariño, ha sido el pilar fundamental en mi vida que me ha ayudado en la buenas y en las malas a ser una padre ejemplar y a lograr mis objetivos sin impórtale mi forma de ser, le agradezco infinitamente.

A mi hija Dayha que me ha enseñado el verdadero sentido de ser padre y gracias a su amor de hija me ha dado el aliento a ser un ejemplo para ella e inculcarle valores que le ayuden en el desarrollo de su vida.

Y por último a todos mis familiares que me brindaron su cariño y apoyo en la consecución de tan grande objetivo

SANTIAGO VILATUÑA CÁRDENAS

AGRADECIMIENTOS

Especialmente a Dios que gracias a sus bendiciones tengo la oportunidad de demostrar a mi familia que con fe y humildad puedo llegar lejos.

Agradezco a mis padres que me inculcaron buenos valores para ser un hombre de bien y creyeron en mi para poder lograr culminar este gran objetivo.

A mi esposa que me aguanto todo este tiempo y no dudo nunca en brindarme su apoyo, conocimiento, cariño y amor con el fin de culminar con este objetivo tan grande.

A mis familiares y amigos que me brindaron su tiempo y apoyo para la consecución de mi objetivo.

A mis Directores de Tesis Ing. Arturo de la Torre e Ing. Victor Páliz, en especial al Director de carrera Ing. Mauricio Campaña los cuales supieron guiarme con sus sabios conocimientos a la consecución de este objetivo.

SANTIAGO VILATUÑA CÁRDENAS

ÍNDICE DE CONTENIDOS

LISTADOS DE TABLAS

RESUMEN

Fideval S.A. Administradora de Fondos y Fideicomisos es una compañía legalmente inscrita en el registro de mercado de valores, constituida con el objetivo de administrar negocios fiduciarios (fideicomisos, encargos fiduciarios de terceros), fondos de Inversión y representar a fondos Internacionales. En ella se maneja información sensible la cual se encuentra alojada en los servidores y sistemas de almacenamiento ubicados en la institución, por lo que es necesario que se garantice su confidencialidad, integridad y disponibilidad de la misma. La presente investigación se orienta a la evaluación o diagnóstico de la seguridad informática en Fideval, porque aparte de verificar las falencias, permitirá implementar controles y políticas en base a las recomendaciones obtenidas para minimizar en el futuro que ocurran estos problemas, y como una forma de prevención para el tratamiento adecuado de datos en riesgos y el cuidado de la información. Cabe señalar que dicho trabajo se desarrollará mediante una investigación documental - descriptiva, para la recolección de la datos y se emplearán políticas de seguridad según el estándar para la seguridad de la información ISO 27001, con el fin de identificar vulnerabilidades en los sistemas de la institución, que conlleva a definir riesgos y recomendar que se establezcan medidas de seguridad de la información y se implemente controles para el manejo de riesgos, monitoreo y revisión del desempeño y efectividad de la empresa, considerando el mejoramiento continuo de la misma.

Palabras Clave:

- **GESTIÓN DE RIESGO,**
- **ISO 27001,**
- **SEGURIDAD INFORMÁTICA,**
- **POLÍTICAS DE SEGURIDAD,**
- **VULNERABILIDADES.**

ABSTRACT

Fideval S.A. Trusts Fund Administrator and is a legally registered company in the register of market, established for the purpose of administering trust business (trust, fiduciary commissions from third parties), representing investment funds and international funds. In her sensitive information which is hosted on the servers and storage systems located in the institution it is run, so it is necessary that its confidentiality, integrity and availability of it is guaranteed. This research is aimed at assessing or diagnosing computer security Fideval because apart from verifying the shortcomings, it will implement controls and policies based on the recommendations obtained to minimize future occurrence of such problems, and as a way of appropriate treatment for the prevention of risk data and care information. It should be noted that this work will be developed through a documentary research - descriptive, for the collection of data and security policies will be used as the standard for ISO 27001 security information in order to identify vulnerabilities in the systems of the institution , leading to define risks and recommend safety measures established information and controls for risk management, monitoring and reviewing the performance and effectiveness of the company is implemented, considering the continuous improvement of the same.

Key Words:

- **RISK MANAGENMENT,**
- **ISO 27001,**
- **INFORMATION SECURITY,**
- **SECURITY POLICIES,**
- **VULNERABILITIES.**

INTRODUCCIÓN

La presente investigación que a continuación se describe, se denomina ¨Gestión de Riesgos Informáticos en la empresa Fideval utilizando ISO 27001¨. Es un trabajo investigativo donde se realiza la evaluación o diagnóstico de la seguridad informática en la empresa Fideval, analizando los riesgos a partir de la norma ISO 27001, lo que nos permite la identificación de las distintas amenazas y vulnerabilidades que poseen los sistemas, con el objeto de implementar los controles necesarios para mantener la disponibilidad, confidencialidad e integridad en la información y las políticas en base a las recomendaciones obtenidas para minimizar en el futuro que ocurran estos problemas representando una forma de prevención para el tratamiento adecuado de datos y el cuidado de la información.

Esta investigación se compone de cinco capítulos, que dentro de su desarrollo se indica en forma coherente todo el proceso llevado a cabo.

El capítulo 1, corresponde a la INTRODUCCIÓN, y contiene la contextualización, la línea de investigación, el árbol de problemas, el análisis crítico, la prognosis, la formulación del problema, la delimitación, la justificación, los objetivos generales y específicos y el alcance del proyecto.

El capítulo 2, corresponde al MARCO TEÓRICO, que contiene los antecedentes de investigación, dividido por seis epígrafes y sus respectivos fundamentos. Los nombres de estos epígrafes a los cuales se hace referencia en este capítulo son:

1. Estándares de Gestión de Seguridad Informática
2. ISO 270001
3. Alcance
4. Términos y Definiciones
5. Sistema de Gestión de Seguridad de la información y
6. La Responsabilidad de la gerencia.

El capítulo 3, corresponde a los pasos a seguir para implementar la norma ISO 27001 en la empresa Fideval.

El capítulo 4, corresponde a la GESTIÓN DE RIESGOS, en el cual se identifican los activos, las principales amenazas, vulnerabilidades e impacto y por último se definen todos los riesgos críticos y se aplica un plan de seguridad adecuado para mitigar los mismos.

El capítulo 5, corresponde a las CONCLUSIONES Y RECOMENDACIONES, en el que se indica las conclusiones y las recomendaciones a las que se llegó en esta investigación.

Finalmente se adjunta la BIBLIOGRAFÍA en la que se apoyó para el desarrollo de esta investigación.

CAPÍTULO 1

INTRODUCCIÓN

1.1 GENERALIDADES

1.1.1 La sociedad de la información

La masificación del uso de ordenadores en las dos últimas décadas provocó un nuevo cambio en la sociedad; vivimos en la sociedad de la información. En la actualidad es difícil concebir nuestra vida sin la asistencia de un ordenador para realizar nuestro trabajo, compartir información con entidades financieras y estatales o disfrutar de momentos de ocio. Más allá de la utilización personal de un ordenador, todas las organizaciones, tanto privadas como estatales sustentan su actividad en el uso de tecnologías informáticas. El desarrollo de las tecnologías informáticas le ha permitido a las organizaciones gestionar de manera muy eficiente el tránsito y almacenamiento de la información

1.1.2 Amenazas informáticas

Si bien es cierto que el desarrollo de las tecnologías informáticas ha permitido un flujo ágil de la información a través de una organización, también es cierto que ha permitido que personas inescrupulosas traten insistentemente de vulnerar el canal por donde fluye la información con el fin de conseguir datos confidenciales de las organizaciones y así obtener ventajas competitivas en el mercado donde se desarrollen las actividades de la empresa víctima como también obtener información delicada de sus funcionarios y clientes.

Peltier clasifica a la amenazas en los siguientes conjuntos (Peltier, 2005, p. 18):

- Amenazas naturales: debidas a la acción de la naturaleza
- Amenazas humanas: eventos que son causados o permitidos por seres humanos

- Amenazas de entorno: debidas a la interacción de la estructura física de un sistema informático con el entorno que le rodea.

1.1.3 Seguridad informática

En respuesta a la presencia de amenazas informáticas en toda organización, nace la necesidad de crear políticas de protección de la información de la organización. Los criterios referentes al tema de la seguridad informática se recogen en varios estándares alrededor del mundo; de estos estándares el más conocido es el ISO 27000; que busca ser un modelo a seguir cuando se requiera gestionar los riesgos informáticos de una organización; en general, estas normas pretenden proveer a cualquier organización, indistintamente de su tamaño y naturaleza, herramientas para implementar y operar un Sistema de Gestión de Seguridad Informática o ISMS por sus siglas en inglés (ISO / IEC, 2009)

1.1.4 Gestión de seguridad de la información

1.1.4.1 Conceptos fundamentales

Tanto ISO 27000 como muchos otros estándares basan su modelo de gestión de riesgos informáticos teniendo en cuenta las mismas consideraciones

- La seguridad de la información y la gestión de riesgos son conceptos son conceptos aplicables a todo tipo de organizaciones: grandes transnacionales, bancos, departamentos de gobierno, instituciones de ayuda humanitaria, hospitales y compañías de seguros; de hecho, toda organización que cree, manipule y transfiera información vital para su operación es apta para aplicar estas ideas.
- Los requerimientos de seguridad y las situaciones en las que los riesgos puedan presentarse van a ser únicas en cada situación pero frecuentemente es posible utilizar enfoques y metodologías comunes.

- La gestión de riesgos es el esfuerzo por equilibrar los posibles ataques que pueda sufrir la organización vs el costo de desplegar las salvaguardas necesarias para mitigarlos.

1.1.4.2 Procedimientos

En general, la gestión de riesgos en tecnologías informáticas se compone de cinco grandes procesos: (Kouns, 2010, pág. 73):

- Identificación de las amenazas, vulnerabilidades y riesgos que tiene un impacto sobre los activos de la organización
- Valoración del riesgo
- Planeación de la mitigación del riesgo
- Implementación de la mitigación del riesgo
- Evaluación de la efectividad de la mitigación

1.1.4.3 Estandarización

Afortunadamente para las partes interesadas de una empresa y los equipos de gestión de riesgo, no tienen que empezar el análisis de riesgos informáticos desde cero, sino que se cuenta con estándares ampliamente aceptados para ayudar en esta tarea. Ya en 1989, el Departamento de Comercio e Industrias del Reino Unido designo un grupo de trabajo para desarrollar el Código de Prácticas de Usuario; más adelante, se destacan los esfuerzos de distintas organizaciones a través de los años 90 por implementar códigos que regulen la gestión de riesgos informáticos; en el año 2000, la Organización Internacional de Estandarización entra en acción al presentar la ISO/IEC 17799: 2000 y un posterior conjunto de estándares referidos a la gestión de riesgos de la información

Análisis de riesgos

El análisis de riesgos comprende la identificación y valoración de amenazas, vulnerabilidades y eventos que tienen el potencial de dañar los activos de una organización (Kouns, 2010, p. 7).

El análisis de riesgos permite a los administradores y encargados de los sistemas informáticos de una organización, conocer las amenazas a las que están expuestos los activos; Además, el análisis de riesgos permite clasificar los activos y sus posibles amenazas de acuerdo al valor que tienen cada uno de ellos.

Valoración de riesgos

“Es el proceso de calcular cuantitativamente el daño potencial y costo monetario causado por una amenaza que tiene impacto sobre un activo informático de la organización” (Kouns, 2010, p. 7).

“Es el computo del riesgo. El riesgo es una amenaza que explota una vulnerabilidad para causar daño sobre un activo. El algoritmo del riesgo computa el riesgo como función de los activos, amenazas y vulnerabilidades” (Peltier, 2005, p. 8).

De los conceptos anteriores se destaca que la valoración de riesgos arroja datos numéricos de los riesgos que indican la cantidad de daño que pueden causar, así como, su impacto económico en la organización. Además se menciona que cálculo del riesgo es función de los activos, amenazas y vulnerabilidades por lo que estos componentes deberán ser expresados también en valores numéricos.

La valoración de riesgos debe ser realizada por un grupo altamente capacitado que se encuentre al tanto de todos los procesos informáticos dentro de la organización, de otro modo se corre el riesgo que esta valoración este errada (Wheeler, 2011, pág. 44)

Mitigación de riesgos

"Mediante este proceso una organización implementa controles y salvaguardas para prevenir la ocurrencia de los riesgos identificados. Al mismo tiempo comprende la implementación de recursos para recuperar los sistemas en caso que los riesgos se materialicen" (Peltier, 2005, p. 8).

La mitigación de riesgos incluye el análisis costo-beneficio, selección, implementación, pruebas y evaluación de seguridad de las salvaguardas (Kouns, 2010, p. 7).

El proceso de mitigación de riesgos incluye el análisis de la factibilidad, eficiencia y costos de las medidas de seguridad y salvaguardas planteadas en base a la valoración de riesgos; además incluye la implementación de las mismas.

Valoración y evaluación de controles de la vulnerabilidad

"Es la examinación sistemática de una infraestructura crítica, de los subsistemas interconectados que la soportan y sus productos para determinar si las medidas de seguridad implementadas son adecuadas, si existe alguna debilidad y evaluar alternativas de implementación" (Peltier, 2005, p. 8).

"Es el monitoreo del sistema para comparar la efectividad contra el conjunto de amenazas, vulnerabilidades y eventos previos, así como el nuevo conjunto de amenazas, vulnerabilidades y eventos derivado de las modificaciones realizadas al sistema" (Kouns, 2010, p. 7)

La valoración y evaluación de los controles de la vulnerabilidad es la etapa de evaluación de las protecciones y salvaguardas implementadas en contra del conjunto de riesgos detectados en primera instancia a fin de determinar su efectividad; asimismo, debido a que es improductivo alcanzar niveles de riesgos nulos, se encarga de evaluar la efectividad de las medidas implementadas en contra del conjunto de riesgos creado a partir del mejoramiento del sistema

1.1.5 Análisis de riesgos

"Análisis de riesgos es una técnica utilizada para identificar y valorar factores que podrían poner en riesgo el éxito de un proyecto el alcanzar una meta" (Peltier, 2005, p. 15).

El análisis de riesgos puede considerarse como un estudio de factibilidad que realiza organización antes de ejecutar los procedimientos prácticos de la gestión de riesgos informáticos. Por tanto, tal y como se expresa en (Peltier, 2005, p. 15), parte de este análisis implica un estudio costo-beneficio de la implementación del sistema de salvaguardas así como la no implementación del mismo; además el autor manifiesta que otro aspecto de este análisis es el impacto que tendrán las salvaguardas sobre los funcionarios de la organización y los clientes

1.1.6 Valoración del riesgo

"Las organizaciones utilizan la valoración de riesgos para determinar qué amenazas existen sobre un activo específico y el nivel de riesgo asociado a dicha amenaza" (Peltier, 2005, p. 16).

La valoración de riesgos comprende el primer conjunto de procedimientos prácticos en la gestión de riesgos informáticos; los procedimientos desarrollados permitirán determinar cuantitativamente el nivel de riesgo al que

están sometidos los activos de la empresa; (Peltier, 2005, p. 16) define seis sub-procesos en la valoración del riesgo:

1. Definición de activos
2. Identificación de las amenazas
3. Determinación de la probabilidad de ocurrencia
4. Determinación del impacto de la amenaza
5. Recomendación de controles
6. Documentación

1.1.6.1 Definición de los activos

Como activo debe entenderse a un sistema, aplicación, procedimiento o bien material que tiene valor o relevancia para la organización y que se desea proteger; la definición de los activos debe realizarse en forma precisa ya que de otro modo no se podrán identificar las amenazas (Peltier, 2005, p. 16)

1.1.6.2 Identificación de amenazas

Peltier menciona que “una amenaza se define como un evento indeseado que tiene impacto en los activos de la empresa” (Peltier, 2005, p. 18).

La identificación de amenazas comprende el estudio de las características de los activos de la empresa en busca de situaciones que puedan comprometer su integridad o desarrollo. Peltier agrupa los diferentes tipos de amenazas en tres categorías (Peltier, 2005):

1) Amenazas naturales
2) Amenazas humanas
3) Amenazas del entorno

Amenazas naturales

Se producen por efecto de la madre naturaleza. Por ejemplo tormentas eléctricas, terremotos, erupciones volcánicas, inundaciones, entre otros.

Amenazas humanas

Se deben a la acción del ser humano; la ocurrencia de estos acontecimientos se puede producir por la omisión del personal y usuarios del sistema informático de la empresa al no tener en cuenta las políticas de seguridad o bien por ataques deliberados como pueden ser accesos no autorizados al sistema, ataques con virus informáticos, robo de equipos, entre otros.

Amenazas del entorno

Estas se deben al deterioro de los elementos físicos que conforman el sistema informático con el medio ambiente; ejemplos de este tipo de amenazas son la contaminación por polvo, humedad ambiental, sobretensiones en la línea, oxidación, entre otros.

Determinación de la probabilidad de ocurrencia

Peltier menciona que: “una vez que la elaboración de la lista de amenazas termine, será necesario determinar cuál es la probabilidad de que estas ocurran” (Peltier, 2005, pág. 19).

La determinación de la probabilidad de ocurrencia permitirá asignarle la importancia justa a cada una de las amenazas. La probabilidad de ocurrencia depende en gran medida de naturaleza de la actividad de cada empresa y su ubicación geográfica; por ejemplo, la posibilidad de que la empresa sea alcanzada por un misil es casi nula en Ecuador mientras que en Medio Oriente debe ser alta.

Determinación del impacto de la amenaza

Respecto a la determinación del impacto, Peltier expresa lo siguiente: “impacto es la magnitud de la pérdida de valor de un activo” (Peltier, 2005, pág. 24).

Otro punto de vista respecto al impacto lo expresa Boker de la siguiente manera: “Una amenaza es cualquier cosa que pueda causar daño a los bienes de una organización; el impacto es la representación numérica de la cantidad de daño que puede hacer esta amenaza” (Borek, 2013, pág. 30)

La determinación del impacto es la medida cuantitativa del daño que puede causar una amenaza sobre los activos de la empresa; el valor del impacto de una determinada magnitud dependerá de la naturaleza de la empresa así como el criterio del grupo de trabajo que realice la valoración.

Recomendación de controles

Peltier menciona a propósito de la recomendación de controles que: “después que el nivel de riesgo sea asignado, se deberá identificar los controles o salvaguardas para eliminar el riesgo o al menos reducirlo a un nivel aceptable” (Peltier, 2005, pág. 25).

La determinación del nivel de riesgo de las amenazas identificadas permitirá al grupo de estudio de riesgos plantear las mejores alternativas de control y

salvaguarda de la integridad de los activos de la empresa desde el punto de vista técnico; ejemplos de controles propuestos pueden ser implementación de lectores de huellas dactilares, antivirus, porteros electrónicos, adquisición de cajas fuertes, entre otros..

Documentación

Peltier expresa sobre la documentación que debe recolectarse sobre las actividades realizadas a fin de controlar los riesgos sobre los activos de la organización lo siguiente: “una vez terminado el estudio, los resultados deben ser documentados en un formato estándar y presentados a la administración” (Peltier, 2005, pág. 27).

La documentación del análisis de riesgos permitirá un mejor entendimiento de todos los pasos que se han seguido desde la identificación de los activos hasta la recomendación de los controles. Los documentos generados servirán además como soporte para futuros estudios y como puente de entre el departamento técnico y la administración.

Análisis del costo-beneficio

Es análisis costo beneficio es una herramienta administrativa que permitirá evaluar las ventajas económicas de la implementación de los controles y las salvaguardas recomendadas en el análisis técnico. Si bien ya no es competencia directa del departamento técnico, es necesario nombrarlo ya que constituye la etapa decisiva del proyecto. Peltier recomienda tener en cuenta algunos aspectos a la hora de realizar este análisis (Peltier, 2005, pág. 27):

- Costos de implementación, que incluyen tanto el hardware, el software
- Reducción con el tiempo de la efectividad del sistema

- Implementación de nuevas políticas y procedimientos a fin de sostener los nuevos controles
- Posibilidad de que nuevo personal deba ser contratado o al menos de que una parte del personal actual deba ser capacitado
- Mantenimiento del sistema

1.2 ANTECEDENTES

1.2.1 Fideval S.A.

Fideval S.A. es una empresa dedicada a la administración de fondos y fideicomisos con presencia en el mercado ecuatoriano desde 1998. La empresa ha venido manejando una importante cantidad de dinero en activos de terceros, siendo en la actualidad la principal administradora de fondos y fideicomisos ecuatoriana. La tabla 1.1 muestra la evolución de la empresa a través del tiempo.

Tabla 1:

Evolución de la empresa Fideval S.A. a través del tiempo

Año	Acontecimiento
1998	Creación de la empresa como parte del grupo financiero Arseval
2001	Fideval se independiza de Grupos financieros
2005	Fideval inicia su participación en el proceso de titularización
2009	Fideval inicia su modelo de gestión en administración de fideicomisos masivos
2012	Fideval inicia el proceso de fusión con Fondos Pichincha
2013	Fideval se especializa en fondos de inversión
2014	Fideval lanza el Fondo Fix 90

Tomado de (Fideval, 2014)

Fideval se ha caracterizado por sus esfuerzos en gestionar de manera eficiente la información de todos sus clientes para lo cual cuenta con un equipo completo de profesionales dedicados a desarrollar soluciones informáticas que le permita a los clientes disponer de su información en cualquier lugar del mundo (Fideval, 2014).

1.2.2 Gestión de riesgos informáticos en Fideval S.A.

A pesar de los grandes esfuerzos de la empresa en el área tecnológica, existe una observación importante: debido a que se encuentra en proceso de fusión con Fondos Pichincha, la empresa no cuenta con un sistema de gestión de riesgos informáticos integral ya que en la actualidad cada empresa realiza su propio análisis de riesgos y toma medidas preventivas cada una por su cuenta.

Algunos de los problemas que pueden identificarse dentro de la empresa se mencionan a continuación:

- No existe una valoración de activos en la empresa
- No existen indicadores de las amenazas potenciales sobre los sistemas de información
- No se ha estimado el impacto ni el riesgo informático
- No existe un levantamiento de inventario informático basado en una metodología formal
- No se ha identificado las vulnerabilidades y amenazas de cada uno de los activos del inventario
- Al no identificar vulnerabilidades y amenazas de activos tampoco se cuenta con las salvaguardas, por lo tanto no se pueden calcular los impacto y el riesgo.

1.3 JUSTIFICACIÓN

Con el creciente uso de tecnologías informáticas en empresas que manejan información delicada como es el caso de Fideval S.A., lamentablemente también crece el número de antisociales que pretenden apoderarse de manera ilícita de esta información con el fin de sacar provecho propio y perjudicar a la empresa y sus clientes. La piratería informática debe ser combatida por los especialistas en esta área de cada empresa.

Este proyecto pretende utilizar los conocimientos impartidos en la Carrera de Ingeniería en Sistemas para proveer a la empresa Fideval S.A. de un Sistema de Gestión de Riesgos Informáticos tal, que le permita a la empresa salvaguardar la información delicada que maneja tanto propia como de sus clientes, mantener el flujo de dicha información a través de un canal seguro de comunicación y defenderse de ataques malintencionados oportunamente.

1.4 OBJETIVOS

1.4.1 Objetivo General

Realizar un análisis de riesgos informáticos para disminuir el impacto y el riesgo, mediante el uso del estándar ISO 27001.

1.4.2 Objetivos Específicos

- Catalogar e identificar los activos de la empresa Fideval S.A.
- Identificar las vulnerabilidades y amenazas de los activos de la empresa Fideval S.A.
- Utilizar las técnicas de valoración para el cálculo del impacto y riesgo.
- Elaborar contramedidas que permitan minimizar el impacto y el riego.

1.5 ALCANCE

Este proyecto tiene como objetivo implementar un Sistema de Gestión de Riesgos Informáticos para los sistemas informáticos de la empresa Fideval S.A. para asegurar la integridad, disponibilidad, confidencialidad y control de la información de la empresa y sus clientes.

La metodología a utilizarse en el desarrollo de este proyecto es la descrita por las normas ISO 27000, en especial la norma ISO 27005; esta norma ofrece guías para la gestión de riesgos en la seguridad de la información. Entre las actividades que deben realizarse constan las siguientes:

- Establecimiento del contexto.
- Valoración del riesgo.
- Tratamiento del riesgo.
- Aceptación del riesgo.
- Documentación del riesgo.
- Monitoreo y revisión del riesgo.

Teniendo en cuenta las características de la empresa, y de acuerdo a la normativa antes mencionada, el presente proyecto pretende desarrollar las siguientes actividades:

- Identificación de los activos con mayor riesgo aparente dentro de la empresa FIDEVAL.
- Valoración de los activos de acuerdo al papel que cumplen dentro de la empresa.
- Determinación de las amenazas de acuerdo a cada tipo de activo identificado en el punto anterior.

- Determinación de la frecuencia de ocurrencia de las amenazas sobre los activos.
- Valoración de las amenazas de acuerdo al daño potencial que pueden causar en los activos de la empresa.
- Cálculo del impacto y riesgo de los activos.
- Determinación de las salvaguardas a implementarse.
- Determinación de la eficacia de las salvaguardas.
- Cálculo del impacto y riesgo residual.
- Análisis de los resultados del punto anterior.
- Elaboración de un plan de mejoramiento de seguridad en la información para la empresa FIDEVA S.A.
- Análisis final de los resultados del proyecto.

CAPÍTULO 2

MARCO TEÓRICO

2.1 ESTÁNDARES DE GESTIÒN DE SEGURIDAD INFORMÀTICA

La seguridad de la información y la gestión de riesgos son conceptos aplicables a todo tipo de organizaciones: grandes transnacionales, bancos, departamentos de gobierno, instituciones de ayuda humanitaria, hospitales y compañías de seguros; de hecho, toda organización que cree, manipule y transfiera información vital para su operación es apta para aplicar estas ideas. Los requerimientos de seguridad y las situaciones en las que los riesgos puedan presentarse van a ser únicas en cada situación pero frecuentemente es posible utilizar enfoques y metodologías comunes. La gestión de riesgos es el esfuerzo por equilibrar los posibles ataques que pueda sufrir la organización con los costó de desplegar las salvaguardas necesarias para mitigarlos.

En general, la gestión de riesgos en tecnologías informáticas se compone de cinco grandes procesos: (Kouns, 2010, pág. 73):

1. Identificación de las amenazas, vulnerabilidades y riesgos que tiene un impacto sobre los activos de la organización.
2. Valoración del riesgo.
3. Planeación de la mitigación del riesgo.
4. Implementación de la mitigación del riesgo.
5. Evaluación de la efectividad de la mitigación.

Afortunadamente para las partes interesadas de una empresa y los equipos de gestión de riesgo, no tienen que empezar el análisis de riesgos informáticos desde cero sino que se cuenta con estándares ampliamente aceptados para ayudar en esta tarea. Ya en 1989, el Departamento de Comercio e Industrias del Reino Unido designó un grupo de trabajo para desarrollar el Código de Prácticas de Usuario; más adelante, se destacan los esfuerzos de distintas organizaciones a través de los años 90 por implementar códigos que regulen la gestión de riesgos informáticos; en el año 2000, la Organización Internacional de Estandarización entra en acción al presentar la ISO/IEC 17799: 2000 y un posterior conjunto de estándares referidos a la gestión de riesgos de la información.

British Standards Institute (BSI)	1. BS7799-1:1999, ‘‘Código de prácticas para la gestión de seguridad informática’’ fue retirado con la aparición de ISO/IEC 17799:2000. 2. BS7799-2:2002 fue la más reciente especificación que lanzo la BSI en materia de seguridad informática. Después de la aparición de la ISO/IEC 17799:2005, fue rápidamente asimilada por ISO/IEC 27001:2005 3. BS7799-3:2006, ‘‘Guías para los sistemas de gestión de riesgos informáticos’’. Este estándar provee lineamientos y soportes para la implementación de procesos de gestión de riesgos y es lo suficientemente genérico para ser utilizado en medianas y grandes organizaciones. Algunas de sus cláusulas incluyen: • Seguridad de la información en el contexto de la organización • Valoración del riesgo • Tratamiento del riesgo y gestión de la toma de decisiones • Actividades de gestión de riesgo sobre la marcha • Ejemplos de conformidad legal y regulatoria • Riesgos de información y riesgos organizacionales • Ejemplos de bienes, amenazas, vulnerabilidades y valoración del riesgo • Herramientas de gestión de riesgo • Compaginación con las normas ISO/IEC 27001:2005 and BS7799-3:2006

International Organization for Standardization (ISO)	1. ISO/IEC 13335-1:2004, “Tecnología de la información—Técnicas de seguridad—Gestión de la seguridad de la información y tecnologías de la comunicación”. Este estándar contiene Conceptos y modelos comúnmente aceptados para la gestión de la seguridad de la información y tecnologías de la comunicación 2. Familia de normas para la gestión de riesgos informáticos ISO 27000 (también conocido como “ISO27k”). Los estándares más representativos de esta familia son: ISO/IEC 27002, ISO/IEC 27005 3. ISO/IEC 18028:2006, Información tecnológica—técnicas de seguridad—Redes de seguridad de la tecnologías de la información”. Las cinco partes de este estándar contiene lineamientos en materia de gestión de la seguridad, operación y uso de redes de información tecnológica; este estándar puede considerarse como una extensión de las normas ISO/IEC 13335 y ISO/IEC 17799 enfocado en riesgos de redes informáticas 4. ISO/IEC TR 18044: 2004, “Tecnología de la información—Técnicas de seguridad—Gestión de incidentes en la seguridad de la información”. Provee, en parte, información de los beneficios obtenidos de un buen enfoque de la gestión de incidentes en seguridad informática así como lineamientos para el desarrollo del proceso de gestión de incidentes en seguridad informática

2.1.1 ISO/IEC 13335

ISO 13335 (originalmente un conjunto de reportes técnicos) es un conjunto de lineamientos para la gestión de riesgos informáticos, enfocado en controles de medición de seguridad técnica. El estándar está compuesto de cuatro partes, donde la primera parte identifica el proceso completo y muestra los diferentes componentes necesarios para completar una valoración del riesgo

2.1.1.1 ISO/IEC 13335-1

La ISO/IEC 13335-1 comprende conceptos y modelos de gestión de la seguridad de la información y tecnologías de comunicación; esta sección presenta los modelos y conceptos fundamentales para un entendimiento básico de la seguridad en tecnologías de la información y comunicación (TIC) y el direccionamiento general de la gestión a fin de conseguir una eficiente planeación, implementación y operación de las seguridades de las TIC; en esta parte del estándar se explica el concepto fundamental de seguridad; seguidamente se explican las políticas y principios necesarios para la implementación de una estructura de seguridad y finalmente se explica la función de la administración y la gestión de riesgos dentro de la organización

2.1.1.2 ISO/IEC 13335-2

Provee los lineamientos operacionales para la implementación de un marco de seguridad sobre tecnologías de información y comunicación

2.1.2 ISO 27000

ISO 27000 es una familia de estándares desarrollados en conjunto por la Organización Internacional de Estandarización (ISO) y la Comisión Internacional Electrotécnica (IEC) en el afán de proveer un marco referencial de gestión de la información que pueda ser utilizado por cualquier tipo de organización.

2.1.3 Estándares más relevantes de ISO 27000

2.1.3.1 ISO 27000

Contiene los lineamientos generales de cada uno de los estándares que componen la familia ISO 27000; además, fundamenta la importancia de la implementación de los SGSI (Sistemas de Gestión de Seguridad de la información) y provee una breve descripción de los pasos para el establecimiento, monitorización mantenimiento y mejora de un SGSI

2.1.3.1.1 Términos y definiciones

La siguiente terminología aplica a esta norma:

- **Activo:** se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.
- **Aceptación de Riesgos:** Decisión de aceptar un riesgo.
- **Análisis de Riesgo:** Uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Administración del Riesgo:** Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.
- **Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados.
- **Disponibilidad:** Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.
- **Declaración de Aplicabilidad:** documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos, además de la justificación tanto de su selección como de la exclusión de controles incluidos en el ANEXO A.

- **Evaluación de riesgos:** Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- **Incidente de Seguridad:** Evento único o serie de eventos de seguridad de la información inesperada o no deseada que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de información.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Riesgo Residual:** el riesgo que permanece tras el tratamiento de riesgos.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.
- **Eventos de Seguridad de la Información:** Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior o desconocida que podría ser relevante para la seguridad.
- **Tratamiento de Riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo.
- **Valoración de Riesgos:** Proceso Completo de análisis y evaluación de riesgos.

2.2 ISO 27001

Este estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple. (ISO 27000 en español, 2014)

Este Estándar Internacional puede ser utilizado por entidades internas y externas para evaluar la conformidad.

2.2.1 Enfoque del Proceso

Este Estándar Internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de Insumos en outputs, se puede considerar un proceso. Con frecuencia el output de un proceso forma directamente el Insumo del siguiente proceso.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un ‘enfoque del proceso’.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
- Implementar y operar controles para manejar los riesgos de la seguridad de la información;
- Monitorear y revisar el desempeño y la efectividad del SGSI; y
- Continuo mejoramiento en base a la medición del objetivo.

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. La Figura 1 muestra cómo un SGSI toma como Insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas.

La adopción del modelo PDCA también reflejará los principios tal como se establecen en los Lineamientos OECD (2002) que gobiernan los sistemas y redes de seguridad de la información.

Este Estándar Internacional proporciona un modelo sólido para implementar los principios en aquellos lineamientos que gobiernan la evaluación del riesgo, diseño e implementación de seguridad, gestión y re-evaluación de la seguridad.

A continuación se desarrollan los conceptos principales del PDCA:

- **Planear**

  Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

- **Hacer**

  Implementar y operar la política, controles, procesos y procedimientos SGSI.

- **Chequear**

  Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.

- **Actuar**

  Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI (Organización Internacional de Estandarización, 2005, pág. 15)

2.2.2 Compatibilidad con otros sistemas de gestión

Este Estándar Internacional se alinea con el ISO 9001:2000 e ISO 14001:2004 para dar soporte a una implementación y operación consistente e integrada con los estándares de gestión relacionados. Por lo tanto, un sistema

de gestión adecuadamente diseñado puede satisfacer los requerimientos de todos estos estándares. Este Estándar Internacional está diseñado para permitir que una organización se alinee o integre su SGSI con los requerimientos del sistema de gestión relacionado (ISO 27000 en español, 2014, pág. 10)**.**

2.3 ALCANCE

2.3.1 General

Este Estándar Internacional abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro).

Este Estándar Internacional especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.

El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas. (Organización Internacional de Estandarización, 2005, pág. 5)

2.3.2 Aplicación

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza. No es aceptable la exclusión de ninguno de los requerimientos especificados en las Cláusulas 4, 5, 6, y 8 cuando una organización asegura su conformidad con este Estándar Internacional.

Cualquier exclusión de los controles vista como necesaria para satisfacer el criterio de aceptación del riesgo tiene que ser justificada y se debe proporcionar evidencia de que los riesgos asociados han sido aceptados por las personas responsables. Cuando se realizan exclusiones, las aseveraciones de conformidad con este estándar no son aceptables a no ser que estas exclusiones no afecten la capacidad y/o responsabilidad de la organización, para proporcionar seguridad de la información que satisfaga los requerimientos de seguridad determinados por la evaluación de riesgo y los requerimientos reguladores aplicables. (Organización Internacional de Estandarización, 2005, pág. 7)

2.4 TÉRMINOS Y DEFINICIONES

Para propósitos de este documento, se aplican los siguientes términos y definiciones:

- **Activo**

  Cualquier cosa que tenga valor para la organización (ISO/IEC 13335-1:2004).

- **Disponibilidad**

  La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC 13335-1:2004).

- **Confidencialidad**

  La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados (ISO/IEC 13335-1:2004).

- **Seguridad de información**

  Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad (ISO/IEC 17799:2005).

- **Evento de seguridad de la información**

  Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad. (ISO/IEC TR 18044:2004).

- **Incidente de seguridad de la información**

  Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información. (ISO/IEC TR 18044:2004).

- **Sistema de gestión de seguridad de la información SGSI**

  Esa parte del sistema gerencial general está basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

  NOTA: El sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos. (Organización Internacional de Estandarización, 2005, pág. 8).

- **Integridad**

  La propiedad de salvaguardar la exactitud e integridad de los activos. (ISO/IEC 13335-1:2004).

- **Riesgo residual**

  El riesgo remanente después del tratamiento del riesgo (ISO/IEC Guía 73:2002).

- **Aceptación de riesgo**

  Decisión de aceptar el riesgo (ISO/IEC Guía 73:2002)

- **Análisis de riesgo**

  Uso sistemático de la información para identificar fuentes y para estimar el riesgo.
  (ISO/IEC Guía 73:2002).

- **Valuación del riesgo**

  Proceso general de análisis del riesgo y evaluación del riesgo (ISO/IEC Guía 73:2002).

- **Evaluación del riesgo**

  Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo (ISO/IEC Guía 73:2002).

- **Gestión del riesgo**

  Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
  (ISO/IEC Guía 73:2002).

- **Tratamiento del riesgo**

  Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo (ISO/IEC Guía 73:2002)

  NOTA: En este Estándar Internacional el término ‘control’ se utiliza como sinónimo de ‘medida’.

- **Enunciado de aplicabilidad**

  Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.

  NOTA: Los objetivos de control y controles se basan en los resultados y conclusiones de los procesos de tasación del riesgo y los procesos de tratamiento del riesgo, los requerimientos legales o reguladores, las obligaciones contractuales y los requerimientos comerciales de la organización para la seguridad de la información.

2.5 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

2.5.1 Requerimientos generales

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan.

2.5.2 Establecer y manejar el SGSI

2.5.2.1 Establecer el SGSI

La organización debe hacer lo siguiente:

- Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e

incluyendo los detalles de y la justificación de cualquier exclusión del alcance

- Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología que:
    - Incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información;
    - Tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual;
    - Esté alineada con el contexto de la gestión riesgo estratégico de la organización en el cual se dará el establecimiento y mantenimiento del SGSI;
    - Establezca el criterio con el que se evaluará el riesgo
    - Haya sido aprobada por la gerencia.
- Definir el enfoque de valuación del riesgo de la organización
    - Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.
    - Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables. (Organización Internacional de Estandarización, 2005, pág. 11)

La metodología de estimación del riesgo seleccionada debe asegurar que los cálculos del riesgo produzcan resultados comparables y reproducibles.

- Identificar los riesgos
    - Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos.
    - Identificar las amenazas para aquellos activos.
    - Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.
    - Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

- Analizar y evaluar el riesgo
    - Calcular el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.
    - Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.
    - Calcular los niveles de riesgo.
    - Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido en 4.2.1 (c) (2).
- Identificar y evaluar las opciones para el tratamiento de los riesgos

  Las acciones posibles incluyen:
    - Aplicar los controles apropiados;
    - Aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo de la organización;

- Evitar los riesgos; y
- Transferir los riesgos comerciales asociados a otras entidades; por ejemplo: aseguradoras, proveedores.

- Seleccionar objetivos de control y controles para el tratamiento de riesgos

Se deben seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento del riesgo. Esta selección debe tomar en cuenta el criterio para aceptar los riesgos, así como los requerimientos legales, reguladores y contractuales.

Se deben seleccionar los objetivos de control y los controles del Anexo A como parte de este proceso conforme sea apropiado para cubrir estos requerimientos.

Los objetivos de control y controles listados en el Anexo A no son exhaustivos y también se pueden seleccionar objetivos de control y controles adicionales. (Organización Internacional de Estandarización, 2005, pág. 15)

- Obtener la aprobación de la gerencia para los riesgos residuales propuestos.
- Obtener la autorización de la gerencia para implementar y operar el SGSI.
- Preparar un Enunciado de Aplicabilidad.

  Se debe preparar un Enunciado de Aplicabilidad que incluya lo siguiente:

- Los objetivos de control y los controles seleccionados en y las razones para su selección.
- Los objetivos de control y controles implementados actualmente.

2.5.2.2 Implementar y operar el SGSI

La organización debe hacer lo siguiente:

- Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.
- Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.
- Implementar los controles seleccionados en el apartado anterior para satisfacer los objetivos de control.
- Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control para producir resultados comparables y reproducibles.
- Implementar los programas de capacitación y conocimiento.
- Manejar las operaciones del SGSI.
- Manejar recursos para el SGSI.
- Implementar los procedimientos y otros controles capaces de permitir una pronta detección de y respuesta a incidentes de seguridad. (Organización Internacional de Estandarización, 2005, pág. 16).

2.5.2.3 Monitorear y revisar el SGSI

La organización debe hacer lo siguiente:

- Ejecutar procedimientos de monitoreo y revisión, y otros controles para:
    - Detectar prontamente los errores en los resultados de procesamiento;
    - Identificar prontamente los incidentes y violaciones de seguridad fallidos y exitosos;
    - Permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaba;
    - Ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores; y
    - Determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.
- Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorías de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.
- Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
- Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:

- La organización;
- Tecnología;
- Objetivos y procesos comerciales;
- Amenazas identificadas;
- Efectividad de los controles implementados; y
- Eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.
- Realizar auditorías SGSI internas a intervalos planeados.

- Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI.
- Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.
- h) Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI. (Organización Internacional de Estandarización, 2005, pág. 17)

2.5.2.4 Mantener y mejorar el SGSI

La organización debe realizar regularmente lo siguiente:

- Implementar las mejoras identificadas en el SGSI.
- Tomar las acciones correctivas y preventivas apropiadas en concordancia con 8.2 y 8.3.
- Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.
- Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias relevantes
- Asegurar que las mejoras logren sus objetivos señalados.

2.5.3 Requerimientos de documentación

2.5.3.1 General

La documentación debe incluir los registros de las decisiones gerenciales, asegurar que las acciones puedan ser monitoreadas a las decisiones y políticas gerenciales, y los resultados registrados deben ser reproducibles.

Es importante ser capaces de demostrar la relación desde los controles seleccionados y de regreso a los resultados del proceso de evaluación del riesgo y tratamiento del riesgo, y subsecuentemente, de regreso a la política y objetivos del SGSI.

La documentación SGSI debe incluir lo siguiente:

- Enunciados documentados de la política SGSI y los objetivos;
- El alcance del SGSI;
- Procedimientos y controles de soporte del SGSI;
- Una descripción de la metodología de evaluación del riesgo;
- Reporte de evaluación del riesgo;
- Plan de tratamiento del riesgo;
- Los procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles;
- Registros requeridos por este Estándar Internacional.
- Enunciado de Aplicabilidad.

NOTA 1: Cuando aparece el término ‘procedimiento documentado’ dentro este Estándar Internacional, significa que el procedimiento se establece, documenta, implementa y mantiene.

NOTA 2: La extensión de la documentación SGSI puede diferir de una organización a otro debido a:

- el tamaño de la organización y el tipo de sus actividades; y
- el alcance y complejidad de los requerimientos de seguridad y el sistema que se está manejando.

NOTA 3: Los documentos y registros pueden estar en cualquier forma o medio.

2.5.3.2 Control de documentos

Los documentos requeridos por el SGSI deben ser protegidos y controlados. Se debe establecer un procedimiento documentado para definir las acciones gerenciales necesarias para:

- Aprobar la idoneidad de los documentos antes de su emisión;
- Revisar y actualizar los documentos conforme sea necesario y re-aprobar los documentos;
- Asegurar que se identifiquen los cambios y el status de la revisión actual de los documentos
- Asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso;
- Asegurar que los documentos se mantengan legibles y fácilmente identificables;
- Asegurar que los documentos estén disponibles para aquellos que los necesitan; y sean transferidos, almacenados y finalmente eliminados en concordancia con los procedimientos aplicables para su clasificación;

- Asegurar que se identifiquen los documentos de origen externo;
- Asegurar que se controle la distribución de documentos;
- Evitar el uso indebido de documentos obsoletos; y
- Aplicarles una identificación adecuada si se van a retener por algún propósito.

2.5.3.3 Control de registros

Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Deben ser protegidos y controlados. El SGSI debe tomar en cuenta cualquier requerimiento legal o regulador relevante. Los registros deben mantenerse legibles, fácilmente identificables y recuperables. Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros. (Organización Internacional de Estandarización, 2005, pág. 18)

2.6 RESPONSABILIDAD DE LA GERENCIA

2.6.1 Compromiso de la gerencia

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI al:

- Establecer una política SGSI;
- Asegurar que se establezcan objetivos y planes SGSI;
- Establecer roles y responsabilidades para la seguridad de información;
- Comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de un mejoramiento continuo;

- Proporcionar los recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI;
- Decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptables;
- Asegurar que se realicen las auditorías internas SGSI; y
- Realizar revisiones gerenciales del SGSI

2.6.2 Gestión de recursos

2.6.2.1 Provisión de recursos

La organización debe determinar y proporcionar los recursos necesarios para:

- Establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI;
- Asegurar que los procedimientos de seguridad de la información respalden los requerimientos comerciales;
- Identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales;
- Mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados;
- Llevar a cabo revisiones cuando sean necesarias, y reaccionar apropiadamente ante los resultados de estas revisiones;
- Donde se requiera, mejorar la efectividad del SGSI.

2.6.2.2 Capacitación, conocimiento y capacidad

La organización debe asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas para:

- Determinar las capacidades necesarias para el personal que realiza trabajo que afecta el SGSI;
- Proporcionar la capacitación o realizar otras acciones (por ejemplo; emplear el personal competente) para satisfacer estas necesidades;
- Evaluar la efectividad de las acciones tomadas;
- Mantener registros de educación, capacitación, capacidades, experiencia y calificaciones.

La organización también debe asegurarse que todo el personal relevante esté consciente de la relevancia e importancia de sus actividades de seguridad de la información y cómo ellos pueden contribuir al logro de los objetivos SGSI.

2.7 AUDITORÍAS INTERNAS SGSI

La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI:

- Cumplen con los requerimientos de este Estándar Internacional y la legislación y regulaciones relevantes;
- Cumplen con los requerimientos de seguridad de la información identificados;
- Se implementan y mantienen de manera efectiva;
- Se realizan conforme lo esperado.

Se debe planear un programa de auditoría tomando en consideración el status e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas. Se debe definir el criterio, alcance, frecuencia y métodos de auditoría. La selección de los auditores y la

realización de las auditorías deben asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

Las responsabilidades y requerimientos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros se deben definir en un procedimiento documentado.

La gerencia responsable para el área siendo auditada debe asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación.

2.8 REVISIÓN GENERAL DEL SGSI

2.8.1 General

La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información. Los resultados de las revisiones deben documentarse claramente y se deben mantener registros.

2.8.2 Insumo de la revisión

El insumo para la revisión gerencial debe incluir:

- Resultados de auditorías y revisiones del SGSI;
- Retroalimentación de las partes interesadas;
- Técnicas, productos o procedimientos, que se podrían utilizar en la organización para mejorar el desempeño y efectividad del SGSI;
- Estatus de acciones preventivas y correctivas;

- Vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa;
- Resultados de mediciones de efectividad;
- Acciones de seguimiento de las revisiones gerenciales previas;
- Cualquier cambio que pudiera afectar el SGSI;
- Recomendaciones para el mejoramiento. (Organización Internacional de Estandarización, 2005, pág. 18).

2.8.3 Resultado de la revisión

El resultado de la revisión gerencial debe incluir cualquier decisión y acción relacionada con lo siguiente:

- Mejoramiento de la efectividad del SGSI;
- Actualización de la evaluación del riesgo y el plan de tratamiento del riesgo;
- Modificación de procedimientos y controles que afectan la seguridad de la información, si fuese necesario, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI, incluyendo cambios en:
    - Requerimientos comerciales;
    - Requerimientos de seguridad;
    - Procesos comerciales que afectan los requerimientos comerciales existentes;
    - Requerimientos reguladores o legales;
    - Obligaciones contractuales; y
    - Niveles de riesgo y/o criterio de aceptación del riesgo.
- Necesidades de recursos;
- Mejoramiento de cómo se mide la efectividad de los controles

2.9 MEJORAMIENTO DEL DEL SGSI

2.9.1 Mejoramiento continuo

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoria, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.

2.9.2 Acción correctiva

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requerimientos del SGSI para poder evitar la recurrencia. El procedimiento documentado para la acción correctiva debe definir los requerimientos para:

- Identificar las no-conformidades;
- Determinar las causas de las no-conformidades;
- Evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir;
- Determinar e implementar la acción correctiva necesaria;
- Registrar los resultados de la acción tomada;
- Revisar la acción correctiva tomada.

2.9.3 Acción preventiva

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requerimientos SGSI para evitar su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requerimientos para:

- Identificar las no-conformidades potenciales y sus causas;
- Evaluar la necesidad para la acción para evitar la ocurrencia de no-conformidades;
- Determinar e implementar la acción preventiva necesaria;
- Registrar los resultados de la acción tomada
- Revisar la acción preventiva tomada.

La organización debe identificar los riesgos cambiados e identificar los requerimientos de acción preventiva enfocando la atención sobre los riesgos cambiados significativamente.

La prioridad de las acciones preventivas se debe determinar en base a los resultados de la evaluación del riesgo.

NOTA La acción para evitar las no-conformidades con frecuencia es más una acción efectiva en costo que la acción correctiva. (Organización Internacional de Estandarización, 2005, pág. 20)

2.10 Anexo A: OBJETIVOS DE CONTROL Y CONTROLES

Los objetivos de control y los controles enumerados a continuación se derivan directamente de, y se alinean con, aquellos enumerados en BS ISO/IEC 17799:2005 Cláusulas del 5 al 15. Cada cláusula contiene un número de categorías de seguridad principales. Las once cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son (Organización Internacional de Estandarización, 2005, pág. 30):

- Política de Seguridad (1);
- Organización de la Seguridad de la Información (2);
- Gestión de Activos (2);
- Seguridad de Recursos Humanos (3);

- Seguridad Física y Ambiental (2);
- Gestión de Comunicaciones y Operaciones (10);
- Control de Acceso (7);
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información (6);
- Gestión de Incidentes de Seguridad de la Información (2);
- Gestión de la Continuidad Comercial (1);
- Conformidad (3).

Los controles más importantes para el desarrollo de este proyecto se describen a continuación.

2.10.1 Política de seguridad

2.10.1.1 Política de seguridad de la información

Objetivo: Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

La gerencia establecerá claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.

2.10.1.2 Documento de la política de seguridad de la información

2.10.1.2.1 Control

El documento de la política de seguridad de la información será aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.

2.10.1.2.2 Lineamiento de implementación

El documento de la política de seguridad de la información requiere enunciar el compromiso de la gerencia y establecer el enfoque de la organización para manejar la seguridad de la información. El mismo debe contener enunciados relacionados con:

- Una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información;
- Un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales;
- Un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo;
- Una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización, incluyendo:
    - Conformidad con los requerimientos legislativos, reguladores y restrictivos,
    - Educación, capacitación y conocimiento de seguridad,
    - Gestión de la continuidad del negocio,
    - Consecuencias de las violaciones de la política de seguridad de la información;
    - Una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información,

- Referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios tienen que observar.

Esta política de seguridad de la información necesita comunicar a través de toda la organización a los usuarios en una forma que sea relevante, accesible y entendible para el lector objetivo. (Organización Internacional de Estandarización, 2005, pág. 25).

2.10.1.3 Revisión de la política de seguridad de la información

2.10.1.3.1 Control

La política de seguridad de la información hay que revisarla a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

2.10.1.3.2 Lineamiento de implementación

La política de la seguridad de la información establece tener un dueño que tenga la responsabilidad gerencial aprobada para el desarrollo, revisión y evaluación de la política de seguridad. La revisión incluye las oportunidades de evaluación para el mejoramiento de la política de seguridad de la información de la organización y el enfoque para manejar la seguridad de la información en respuesta a los cambios del ambiente organizacional, circunstancias comerciales, condiciones legales o ambiente técnico.

La revisión de la política de seguridad de la información considera tomar en cuenta los resultados de las revisiones de la gerencia. Deben incluir procedimientos de revisión gerencial y un cronograma o el período de la revisión.

En la entrada para la revisión gerencial incluirá información sobre:

- Retroalimentación de las partes interesadas;
- Resultados de revisiones independientes
- Estado de acciones preventivas y correctivas
- Resultados de revisiones gerenciales previas;
- Desempeño del proceso y conformidad con la política de seguridad de la información;
- Cambios que podrían afectar el enfoque de la organización en el manejo de la seguridad de la información, incluyendo los cambios en el ambiente organizacional; las circunstancias comerciales; la disponibilidad de recursos; condiciones contractuales, reguladoras y legales; o el ambiente técnico;
- Tendencias relacionadas con amenazas y vulnerabilidades;
- Incidentes de seguridad de información reportados
- Recomendaciones provistas por autoridades relevantes

Los outputs de la revisión gerencial incluirá cualquier decisión y acción relacionada con:

- Mejora del enfoque de la organización para manejar la seguridad de la información y sus procesos;
- Mejora de los objetivos de control y los controles;
- Mejora de la asignación de recursos y/o responsabilidades.

Mantener un registro de la revisión gerencial. Obtener la aprobación de la gerencia para la política revisada. (Organización Internacional de Estandarización, 2005, pág. 30)

2.10.2 Organización de la seguridad de la información

2.10.2.1 Organización interna

Objetivo: Manejar la seguridad de la información dentro de la organización.

Establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

La gerencia tendrá la potestad de aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización.

Si fuese necesario, establecer una fuente de consultoría sobre seguridad de la información y estar disponible dentro de la organización. Hay que desarrollar contactos con los especialistas o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado con relación a las tendencias industriales, monitorear los estándares y evaluar los métodos y proporcionar vínculos adecuados para el manejo de los incidentes de seguridad de la información. Fomentar un enfoque multi-disciplinario para la seguridad de la información.

2.10.2.2 Compromiso de la gerencia con la seguridad de la información

2.10.2.2.1 Control

La gerencia apoyará activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.

2.10.2.2.2 Lineamiento de implementación

La gerencia debería:

- Asegurar que los objetivos de seguridad de la información estén identificados, cumplan con los requerimientos organizacionales y estén integrados en los procesos relevantes;
- Formular, revisar y aprobar la política de seguridad de la información;
- Revisar la efectividad de la implementación de la política de seguridad de la información;
- Proporcionar una dirección clara y un apoyo gerencial visible para las iniciativas de seguridad;
- Proporcionar los recursos necesarios para la seguridad de la información;
- Aprobar la asignación de roles y responsabilidades específicas para la seguridad de la información a lo largo de toda la organización;
- Iniciar planes y programas para mantener la conciencia de seguridad de la información;
- Asegurar que la implementación de los controles de seguridad de la información sea coordinado en toda la organización.

La gerencia identificará las necesidades de consultoría especializada interna o externa para la seguridad de la información, y revisar y coordinar los resultados de la consultoría a través de toda la organización.

Dependiendo del tamaño de la organización, estas responsabilidades podrían ser manejadas por un foro gerencial dedicado o por un organismo gerencial existente, como la junta de directores.

2.10.2.3 Coordinación de la seguridad de la información

2.10.2.3.1 Control

Las actividades de la seguridad de la información serán coordinadas por representantes de diferentes partes de la organización con roles y funciones laborales relevantes.

2.10.2.3.2 Lineamiento de implementación

Típicamente, la coordinación de la seguridad de la información tendrá la tarea de involucrar la cooperación y colaboración de los gerentes, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, TI o gestión del riesgo. Esta actividad deberá:

a) asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información;

b) identificar cómo manejar las no-conformidades;

c) aprobar las metodologías y procesos para la seguridad de la información; por ejemplo, la evaluación del riesgo, la clasificación de la información;

d) identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas;

e) evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información;

f) promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización;

g) evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.

Si la organización no utiliza grupos inter-funcionales separados; por ejemplo, porque dicho grupo no es apropiado para el tamaño de la organización; las acciones arriba descritas serán realizadas por otro organismo gerencial adecuado o un gerente individual.

2.10.2.4 Asignación de las responsabilidades de la seguridad de la información

2.10.2.4.1 Control

Todas las responsabilidades de la seguridad de la información estarán claramente definidas.

2.10.2.4.2 Lineamiento de implementación

La asignación de las responsabilidades de la seguridad de la información se realizará en concordancia con la política de seguridad de la información). Se definirá claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos. Cuando sea necesario, esta responsabilidad será complementada con un lineamiento más detallado para locales y medios de procesamiento de información específicos. Se debe definir claramente las responsabilidades locales para la protección de activos y para llevar a cabo procesos de seguridad específicos, como la planeación de la continuidad del negocio.

Las personas con responsabilidades de seguridad asignadas pueden delegar las tareas de seguridad a otros. No obstante, ellos siguen siendo

responsables y determinar si cualquier tarea delegada ha sido realizada correctamente.

Se debe establecer claramente las áreas a las cuales son responsables las diferentes personas; en particular realizar lo siguiente:

- Identificar y definir claramente los activos y procesos de seguridad asociados con cada sistema particular;
- Designar la entidad responsable de cada activo o proceso de seguridad y se documentará los detalles de esta responsabilidad;
- Definir y documentar claramente los niveles de autorización.

2.10.2.5 Autorización de proceso para facilidades procesadoras de información.

2.10.2.5.1 Control

Un proceso de la gerencia para la autorización de facilidades nuevas de procesamiento de información, debe ser definido e implementado.

2.10.2.5.2 Guía de implementación

Las siguientes guías deben ser consideradas para el proceso de autorización:

- Debemos incluir el uso apropiado para solicitar las respectivas autorizaciones gerenciales. Deberá ser obtenida del Gerente responsable del ambiente del sistema de seguridad de información, para asegurar que todas las políticas y requerimientos de seguridad relevantes son cumplidas.
- Donde sea necesario, el hardware y el software ser chequeado para asegurar que son compatibles con otros componentes del sistema.

- El uso de facilidades para el procesamiento de información, bien sean personales o privadas (ejemplo: laptops, computadoras del hogar, sistemas hand-held) pueden introducir nuevas vulnerabilidades y controles necesarios a ser identificados e implementados.

2.10.2.6 Acuerdos de confidencialidad

2.10.2.6.1 Control

Identificar y revisar regularmente que los requerimientos de confidencialidad o acuerdos de no-divulgación reflejan las necesidades de la organización para proteger la información.

2.10.2.6.2 Lineamiento de implementación

En los acuerdos de confidencialidad o no-divulgación hay que tener en cuenta el requerimiento de proteger la información confidencial utilizando términos legalmente ejecutables. Para identificar los requerimientos de los acuerdos de confidencialidad o no-divulgación, se deben considerar los siguientes elementos:

- Una definición de la información a protegerse (por ejemplo, información confidencial);
- Duración esperada de un acuerdo, incluyendo casos donde se podría necesitar mantener la confidencialidad indefinidamente;
- Acciones requeridas cuando se termina un acuerdo;
- Responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada (tal como “sólo lo que necesita saber”);
- Propiedad de la información, secretos comerciales y propiedad intelectual, y cómo se relaciona esto con la protección de la información confidencial;

- Uso permitido de la información confidencial, y los derechos del firmante para utilizar la información;
- Proceso de notificación y reporte de divulgación no autorizada o incumplimiento del acuerdo de información confidencial;
- Condiciones para el retorno o destrucción de la información una vez que se termina el acuerdo; y
- Acciones esperadas a realizarse en caso de incumplimiento de este acuerdo.

En base a los requerimientos de seguridad de la organización, pueden ser necesarios otros elementos en los acuerdos de confidencialidad o no-divulgación.

Los acuerdos de confidencialidad y no-divulgación deben cumplir con todas las leyes y regulaciones aplicables para la jurisdicción en la cual se aplica.

Los requerimientos de los acuerdos de confidencialidad o no-divulgación se deben revisar periódicamente y cuando ocurren cambios que influyen en estos requerimientos.

Puede existir la necesidad que una organización utilice formas diferentes de acuerdos de confidencialidad o no-divulgación en diferentes circunstancias.

2.10.2.7 Contacto con las autoridades

2.10.2.7.1 Control

Mantener los contactos apropiados con las autoridades relevantes.

2.10.2.7.2 Lineamiento de implementación

Las organizaciones tienen que contar con procedimientos que especifiquen cuándo y cuáles autoridades (por ejemplo, policía, departamento de bomberos,

autoridades supervisoras) contactar, y cómo reportar los incidentes de seguridad de la información identificados de una manera oportuna si se sospecha que se han incumplido las leyes.

Las organizaciones atacadas desde le Internet pueden necesitar que terceras personas externas (por ejemplo, un proveedor del servicio de Internet o un operador de telecomunicaciones) tome alguna acción contra la fuente de ataque

2.10.2.8 Contacto con grupos de interés especial

2.10.2.8.1 Control

Mantener contactos apropiados con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

2.10.2.8.2 Lineamiento de implementación

Considerar la membresía en grupos de interés especial como un medio para:

- Increpar el conocimiento sobre las mejores prácticas y mantenerse al día con la información de seguridad relevante;
- Asegurar el entendimiento del ambiente de seguridad de la información sea actualizado y completo.
- Recibir advertencias tempranas de alertas, asesorías y avisos relacionados con ataques y vulnerabilidades;
- Obtener acceso a consultoría especializada de seguridad de la información;
- Compartir e intercambiar información sobre tecnologías, productos, amenazas o vulnerabilidades;
- Proporcionar vínculos adecuados cuando se trata incidentes de seguridad de la información

2.10.2.9 Revisión independiente de la seguridad de la información

2.10.2.9.1 Control

Revisar el enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) de manera independiente a intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.

2.10.2.9.2 Lineamiento de implementación

La gerencia debería iniciar la revisión independiente. Esta revisión independiente es necesaria para asegurar la continua idoneidad, eficiencia y efectividad del enfoque de la organización para manejar la seguridad de la información. La revisión debe incluir las oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el enfoque por seguridad, incluyendo políticas y objetivos de control.

Esta revisión debe ser llevada a cabo por personas independientes al área de revisión; por ejemplo, la función de la auditoria interna, un gerente independiente o una tercera organización especializada en revisiones. Las personas que llevan a cabo estas revisiones necesitan tener la capacidad y experiencia apropiada.

Los resultados de la revisión independiente registrar y reportar a la gerencia que inició la revisión. Mantener estos registros.

Si la revisión independiente identifica que el enfoque y la implementación de la organización para manejar la seguridad de la información no son adecuadas o no cumplen con la dirección para la seguridad de la información establecida en el documento de la política de seguridad de la información.

2.10.2.10 Grupos o personas externas

Objetivo: Mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos.

La seguridad de la información y los medios de procesamiento de la información de la organización no serán reducidos por la introducción de productos y servicios de grupos externos.

Se debe controlar cualquier acceso a los medios de procesamiento de información de la organización y el procesamiento y comunicación de la información realizado por grupos externos.

Cuando existe la necesidad comercial de trabajar con grupos externos que pueden requerir acceso a la información y a los medios de procesamiento de información de la organización, se llevará a cabo una evaluación del riesgo para determinar las implicancias en la seguridad y los requerimientos de control. Acordar y definir los controles en un acuerdo con el grupo externo.

2.10.2.11 Identificación de los riesgos relacionados con los grupos externos

2.10.2.11.1 Control

Identificar los riesgos de la información y los medios de procesamiento de la misma en la organización, a raíz de procesos comerciales que involucran a grupos externos y se implementarán controles apropiados antes de otorgarles acceso.

2.10.2.11.2 Lineamiento de implementación

Donde existe la necesidad de permitir que un grupo externo tenga acceso a los medios de procesamiento de la información o la información de una organización, debemos llevar a cabo una evaluación del riesgo para identificar

cualquier requerimiento de controles específicos. La identificación de los riesgos relacionados con el acceso del grupo externo toma en cuenta los siguientes puntos:

- Los medios de procesamiento de información a los cuales necesita tener acceso el grupo externo;
- El tipo de acceso que tendrá el grupo externo a la información y los medios de procesamiento de la información; por ejemplo;
    - Acceso físico; por ejemplo, oficinas, edificios de cómputo, archivadores;
    - Acceso lógico; por ejemplo, a las bases de datos o sistemas de información de la organización;
    - Conectividad de red entre las redes de la organización y el grupo externo; por ejemplo, conexión permanente, acceso remoto;
    - Si el acceso se da fuera o dentro del local;
- El valor y sensibilidad de la información involucrada, y su grado crítico para las operaciones comerciales;
- Los controles necesarios para proteger la información que no está destinada a ser accesible para los grupos externos;
- El personal del grupo externo involucrado en el manejo de la información de la organización;
- Cómo se puede identificar a la organización y el personal autorizado que tiene acceso, cómo verificar la autorización, y con cuánta frecuencia se necesita reconfirmar esto;
- Los diferentes medios y controles empleados por el grupo externo cuando almacena, procesa, comunica, comparte e intercambia información;

- El impacto del acceso no disponible para el grupo externo cuando lo requiere, y el grupo externo que ingresa o recibe información inexacta o confusa;
- Prácticas y procedimientos para lidiar con los incidentes en la seguridad de la información y los daños potenciales, y los términos y condiciones para la continuación del acceso del grupo externo en caso de un incidente en la seguridad de la información;
- Requerimientos legales, reguladores y otras obligaciones contractuales relevantes que se tomarán en cuenta para el grupo externo;
- Cómo los intereses de cualquier parte interesada pueden verse afectados por los arreglos.

No se puede otorgar acceso a los grupos externos a la información de la organización hasta que se hayan implementado los controles apropiados y, cuando sea factible, se haya firmado un contrato definiendo los términos y condiciones para la conexión o acceso y el contrato de trabajo. Generalmente, todos los requerimientos de seguridad resultantes del trabajo con grupos externos o controles internos se deben reflejar en el acuerdo con el grupo externo.

Se necesita asegurar que el grupo externo esté al tanto de sus obligaciones y acepte las responsabilidades involucradas en tener acceso, procesar, comunicar o manejar la información y los medios de procesamiento de información de la organización.

2.10.2.12 Tratamiento de la seguridad cuando se lidia con clientes

2.10.2.12.1 Control

Es importante tratar todos los requerimientos de seguridad identificados antes de proporcionar a los clientes acceso a la información o activos de la organización.

2.10.2.12.2 Lineamiento de implementación

En esta sección considerar los siguientes términos de seguridad antes de proporcionar a los clientes acceso a cualquier activo de la organización (dependiendo del tipo y extensión de acceso dado, tal vez no se apliquen todos ellos):

- Protección de activos, incluyendo:
  - Procedimientos para proteger los activos de la organización, incluyendo información y software, y el manejo de las vulnerabilidades conocidas;
  - Procedimientos para determinar si algún activo está comprometido; por ejemplo, cuando ha ocurrido una pérdida o modificación de data;
  - Integridad;
  - Restricciones sobre el copiado y divulgación de información;
  - Descripción del producto o servicio a ser provisto;
- Las diferentes razones, requerimientos y beneficios para el acceso del cliente:
- Política de control de acceso, abarcando
  - Métodos de acceso permitidos, y el control y uso de identificadores singulares como IDs del usuario y claves secretas;
  - Un proceso de autorización para el acceso y privilegios del usuario;

  - Un enunciado que establezca que está prohibido todo acceso que no esté explícitamente autorizado;
  - Un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas;
- Acuerdos para el reporte, notificación e investigación de las inexactitudes de la información (por ejemplo, de detalles personales), incidentes de seguridad de información y fallas en la seguridad;
- Una descripción de cada servicio que requieran estar disponible;
- El nivel objetivo del servicio y los niveles inaceptables del servicio;
- El derecho a monitorear, y revocar, cualquier actividad relacionada con los activos de la organización;
- Las respectivas obligaciones de la organización y el cliente;
- Responsabilidades con respecto a temas legales y cómo asegurar que se cumplan los requerimientos legales; por ejemplo, la legislación de protección de data, especialmente tomando en cuenta los diferentes sistemas legales nacionales si el acuerdo involucra cooperación con los clientes en otros países
- Derechos de propiedad intelectual (IPRs) y la asignación de derechos de autor.

2.10.2.13 Tratamiento de la seguridad en acuerdos con terceros

2.10.2.13.1 Control

Los acuerdos de contratos con terceros que involucran el acceso, procesamiento, comunicación, manejo de la información, medios de procesamiento de información de la compañía, o agregan producto y servicios a los medios de procesamiento de información deberán abarcar todos los requerimientos de seguridad relevantes.

2.10.2.13.2 Lineamiento de implementación

El acuerdo requiere asegurar que no existan malos entendidos entre la organización y la otra parte. Las organizaciones deben estar satisfechas con relación a la indemnización de las otras partes.

Se necesita considerar los siguientes términos a incluirse en el acuerdo para cumplir con los requerimientos de seguridad identificados

- La política de seguridad de la información;
- Controles para asegurar la protección de los activos, incluyendo:
    - Procedimientos para proteger los activos organizacionales, incluyendo información, software y hardware;
    - Cualquier control y mecanismo de protección física requerido;
    - Controles para asegurar la protección contra software malicioso
    - Procedimientos para determinar si algún activo está comprometido; por ejemplo, cuando ha ocurrido una pérdida o modificación de data
    - Controles para asegurar el retorno o destrucción de información y los activos al final de, o en un punto de tiempo acordado durante el acuerdo;
    - Confidencialidad, integridad, disponibilidad y cualquier otra propiedad relevante de los activos;
    - Restricciones sobre el copiado y divulgación de información, y la utilización de acuerdos de confidencialidad;
    - Capacitación del usuario y administrador en métodos, procedimientos y seguridad;

- Asegurar la conciencia del usuario para las responsabilidades y problemas de la seguridad de la información;

- Provisión para la transferencia de personal, cuando sea apropiado
- Responsabilidades relacionadas con la instalación y mantenimiento de hardware y software;
- Una estructura de reporte clara y formatos de reporte acordados;
- Un proceso claro y especificado de gestión de cambio;
- Política de control de acceso, abarcando:
    - Las diferentes razones, requerimientos y beneficios que hacen que sea necesario el acceso de terceros;
    - Métodos de acceso permitidos, y el control y uso de identificadores singulares como IDs del usuario y claves secretas;
    - Un proceso de autorización para el acceso y privilegios del usuario;
    - Un requerimiento para mantener una lista de personas autorizadas a utilizar los servicios que se están poniendo a disposición, y los derechos y privilegios con respecto a este uso;
    - Un enunciado que establezca que está prohibido todo acceso que no esté explícitamente autorizado;
    - Un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas;
- Una descripción de cada servicio a estar disponible, y una descripción de la información que mantenga la disponibilidad, junto con su clasificación de seguridad
- El nivel objetivo del servicio y los niveles inaceptables del servicio;
- Una definición del criterio del desempeño verificable, su monitoreo y reporte;
- El derecho a monitorear, y revocar, cualquier actividad relacionada con los activos de la organización;

- El derecho de auditar las responsabilidades definidas en el acuerdo, el derecho que un tercero lleve a cabo la auditoria, y enumerar los derechos estatutarios de los auditores;
- el establecimiento de un proceso escalonado para la solución de problemas;
- Requerimientos de continuidad del negocio, incluyendo las medidas de disponibilidad y confiabilidad, en concordancia con las prioridades comerciales de la organización;
- Las obligaciones respectivas de la organización y el cliente;
- Responsabilidades con respecto a temas legales y cómo asegurar que se cumplan los requerimientos legales; por ejemplo, la legislación de protección de data, especialmente tomando en cuenta los diferentes sistemas legales nacionales si el acuerdo involucra cooperación con los clientes en otros países
- Derechos de propiedad intelectual (IPRs) y la asignación de derechos de autor (Organización Internacional de Estandarización, 2005, pág. 35)

2.10.3 Gestión de activos

2.10.3.1 Responsabilidad por los activos

Objetivo: mantener una apropiada protección de los activos organizacionales. Todos los activos tienen que ser inventariados y contar con un propietario nombrado.

Los propietarios requieren identificar todos los activos y asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos. (Corlleti, 2006, pág. 10)

2.10.3.2 Inventario de los activos

2.10.3.2.1 Control

Identificar todos los activos, elaborar y mantener un inventario de todos los activos importantes.

2.10.3.2.2 Lineamiento de implementación

En una organización hay que identificar todos los activos y documentar la importancia de los mismos. En el inventario de los activos hay que incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial. No debe existir duplicidad de inventarios, pero hay que asegurarse que el contenido esté alineado.

Además, acordar y documentar la propiedad y la clasificación de la propiedad para cada uno de los activos. Basados en la importancia del activo, su valor comercial y su clasificación de seguridad, identificar los niveles de protección que se conmensuran con la importancia de los activos (se puede encontrar más información sobre cómo valorar los activos para representar su importancia en ISO/IEC TR 13335-3.

2.10.3.2.3 Otra información

Existen muchos tipos de activos, incluyendo:

- Información: bases de datos y archivos de data, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoría e información archivada.
- Activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades;

- Activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otro equipo;
- Servicios: servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado;
- Personas, y sus calificaciones, capacidades y experiencia;
- Intangibles, tales como la reputación y la imagen de la organización.

Los inventarios de los activos ayudan a asegurar que se realice una protección efectiva de los activos, y también puede requerir de otros propósitos comerciales; como planes de salud y seguridad, seguros o razones financieras (gestión de activos). El proceso de compilar un inventario de activos es un pre-requisito importante de la gestión del riesgo

2.10.3.3Propiedad de los activos

2.10.3.3.1 Control

Los activos asociados con los medios de procesamiento de información deben ser propiedad de una parte designada de la organización.

2.10.3.3.2 Lineamiento de implementación

El propietario del activo es responsable de:

- Asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente;
- Definir y revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.

La propiedad puede ser asignada a:

- un proceso comercial;
- un conjunto de actividades definido;

- una aplicación;
- un conjunto de data definido.

2.10.3.3.3 Otra información

Se pueden delegar las tareas rutinarias; por ejemplo, a un custodio que supervisa el activo diariamente, pero la responsabilidad permanece con el propietario.

En los sistemas de información complejos podría ser útil designar grupos de activos, los cuales actúan juntos para proporcionar una función particular como "servicios". En este caso el propietario es responsable de la entrega del servicio, incluyendo el funcionamiento de los activos que los proveen. (Organización Internacional de Estandarización, 2005, pág. 40)

2.10.3.4 Uso aceptable de los activos

2.10.3.4.1 Control

Identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.

2.10.3.4.2 Lineamiento de implementación

Todos los empleados, contratistas y terceros necesitan seguir las reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información, incluyendo:

- Reglas para la utilización del correo electrónico e Internet.
- Lineamientos para el uso de dispositivos móviles, especialmente para el uso fuera del local de la organización.

La gerencia relevante proporcionará reglas o lineamientos específicos. Los empleados, contratistas y terceros que usan o tienen acceso a los activos de

la organización deben estar al tanto de los límites existentes para su uso de la información y los activos asociados con los medios y recursos del procesamiento de la información de la organización, hacerse responsables por el uso que le den a cualquier recurso de procesamiento de información, y de cualquier uso realizado bajo su responsabilidad.

2.10.3.5 Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel de protección apropiado.

La información será clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

2.10.3.5.1 Control

Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización.

2.10.3.5.2 Lineamiento de implementación

Las clasificaciones y los controles de protección asociados para la información se tomarán en cuenta las necesidades comerciales de intercambiar o restringir información y los impactos comerciales asociados con dichas necesidades.

En los lineamientos de clasificación incluir protocolos para la clasificación inicial y la re- clasificación a lo largo del tiempo; en concordancia con alguna política pre-determinada de control de acceso

El propietario del activo es responsable de definir la clasificación del mismo, revisarla periódicamente y asegurarse que se mantenga actualizada y en el nivel apropiado.

Tener en consideración el número de categorías de clasificación y los beneficios a obtenerse con su uso. Los esquemas demasiado complejos pueden volverse engorrosos y anti-económicos de utilizar o pueden volverse poco prácticos. Tener cuidado al interpretar los encabezados de la clasificación en los documentos de otras organizaciones, los cuales pueden tener definiciones diferentes para encabezados con el mismo nombre o nombre similares.

2.10.3.5.3 Otra información

Se puede evaluar el nivel de protección analizando la confidencialidad, integridad y disponibilidad, y cualquier otro requerimiento para la información considerada.

Con frecuencia, la información deja de ser sensible o crítica después de cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Hay que tomar en cuenta estos aspectos, ya que la sobre clasificación puede llevar a la implementación de controles innecesarios resultando en un gasto adicional.

Agrupar documentos con requerimientos de seguridad similares cuando se asignan niveles de clasificación podría ayudar a simplificar la tarea de clasificación.

En general, la clasificación dada a la información es una manera rápida para determinar cómo se está manejando y protegiendo la información.

2.10.3.6 Etiquetado y manejo de la información

2.10.3.6.1 Control

Desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información en concordancia con el esquema de clasificación adoptado por la organización.

2.10.3.6.2 Lineamiento de implementación

Los procedimientos para el etiquetado de la información necesitan abarcar los activos de información en formatos físicos y electrónicos.

El output de los sistemas conteniendo información que es clasificada como sensible o crítica deberá llevar la etiqueta de clasificación apropiada. Los ítems a considerarse incluyen reportes impresos, presentaciones en pantalla, medios de grabación (por ejemplo; cintas, discos, CDs), mensajes electrónicos y transferencia de archivos.

Para cada nivel de clasificación definir los procedimientos de manejo seguros; incluyendo el procesamiento, almacenaje, transmisión, de-clasificación y destrucción. Esto también requiere incluir los procedimientos de la cadena de custodia y el registro de cualquier incidente de seguridad relevante.

Los acuerdos con otras organizaciones que incluyen intercambio de información necesitan incluir procedimientos para identificar la clasificación de

esa información e interpretar las etiquetas de clasificación de otras organizaciones.

2.10.3.6.3 Otra información

El etiquetado y el manejo seguro de la información clasificada es un requerimiento clave para los acuerdos de intercambio de información. Las etiquetas físicas son una forma común de etiquetado. Sin embargo, algunos archivos de información, como documentos en forma electrónica, no pueden ser etiquetados físicamente y se necesitan medios electrónicos para el etiquetado. Por ejemplo, la etiqueta de notificación puede aparecer en la pantalla. Cuando no es factible el etiquetado, se pueden aplicar otros medios para designar la clasificación de la información; por ejemplo, mediante procedimientos o meta-data. (Organización Internacional de Estandarización, 2005, pág. 65)

CAPÍTULO 3

IMPLEMENTACIÓN DE LA NORMA ISO 27001

3.1 APLICACIÓN DEL ESTÁNDAR DE SEGURIDAD DE LAINFORMACIÓN ISO 27001

La norma ISO 27001 determina cómo se gestiona la seguridad de la información en una empresa para mitigar los riesgos sobre confidencialidad, integridad y disponibilidad de la misma.

Si no se planifica con atención las actividades de seguridad de la información, es posible que se pase por alto algo importante, lo que se traduce en gastos económicos. Por estos motivos, ISO-27001 afina especialmente en los diferentes pasos de la fase de planificación.

3.1.1 Pasos para implementar la norma ISO 27001

3.1.1.1 Determinar del alcance

Este proyecto se pretende implementar la norma internacional ISO 27001 en la empresa Fideval, asegurando la integridad, disponibilidad, confidencialidad y control de la información de la empresa y sus clientes y culminando con la certificación en la empresa.

3.1.1.2. Determinación de políticas

Las políticas son las reglas generales de comportamiento definidas para la interacción entre los usuarios y los activos informáticos. Estas son independientes de los ambientes propios de la entidad y representan la base de un modelo de seguridad a seguir.

Las políticas deben estar hechas según los requerimientos específicos de cada organización pues dependen de la cultura de cada una de ellas. Por esta razón, en la empresa Fideval, cubrirán los siguientes temas:

Seguridad en la Organización:

- Roles y responsabilidades de seguridad de la información.
- Políticas para la conexión con terceros.

Clasificación de la Información:

- Importancia de la información según la organización.

.

Seguridad en el Recurso Humano:

- Responsabilidades de seguridad de la información para los diferentes cargos.
- Entrenamiento a empleados en seguridad de la información como parte de su proceso de inducción y mejoramiento continuo.

Seguridad Física:

- Control de Acceso Físico.

Administración de las operaciones de cómputo y comunicaciones.

- Políticas sobre el uso del correo electrónico.
- Políticas sobre el uso de Internet.
- Políticas sobre el uso de recursos.
- Control de Acceso.
- Desarrollo y mantenimiento de Sistemas.
- Continuidad de Negocio.

3.1.1.3. Identificar activos, vulnerabilidades y amenazas.

3.1.1.3.1 Identificación de activos

Los activos informáticos o de la información son todos aquellos elementos que sirven de apoyo a la empresa u organización, para ofrecer sus servicios y productos.

La gestión de activos informáticos es uno de los aspectos fundamentales para cualquier empresa u organización. Son necesarios tener en cuenta y valorarlos si se desea implantar un sistema de gestión de la seguridad informática, siguiendo los preceptos de la ISO 27001 (Cano, 2012).

3.1.1.3.1.1 Categorías de activos

A partir de datos extraídos de una reunión planificada con los principales directivos de la empresa Fideval, donde se invitaron los principales colaboradores del departamento de finanzas, se extrajeron una serie de datos, los cuales se consideran imprescindibles para el desarrollo de la presente investigación.

Con esta información se elaboró una matriz para analizar el riego donde se definieron tres clasificaciones de activos (datos, sistemas y personal). La misma se considera como punto clave en analizar y determinar los riesgos en el manejo de los datos e información pues muestra el resultado detallado sobre los riesgos y peligros sobre cada recurso. Ver (Anexo 1-9)

A continuación se presentan las categorías de los activos identificados.

Tabla 2:

Definición de activos.

N°	Activo	Descripción
1	Datos	Datos de riesgo con los que cuenta la empresa Fideval y algunos que navegan en la red.
2	Sistemas	Sistemas que dispone la empresa Fideval, identificados con un determinado riesgo.
3	Personal	Personal por la que está constituida la empresa Fideval.

Estos activos se identificaron con una magnitud de daño atendiendo a cuatro escalas:

- Escala 1: Daño insignificante
- Escala 2: Daño bajo
- Escala 3: Daño mediano
- Escala 4: Daño alto

3.1.1.3.1.1.1 Datos

A continuación se muestran los activos que poseen riesgos en la categoría de Datos. La escala de la magnitud del daño se calculó haciendo un análisis de los riesgos según tres clasificaciones:

Clasificación 1: Confidencial, privado, sensitivo.
Clasificación 2: Obligación por ley, contrato, convenio

Clasificación 3: Costo de recuperación (Tiempo, económico, material, imagen, emocional)

En este informe sólo se hará referencia a los activos que poseen una magnitud de daño mediano y alto para su posterior análisis por la importancia que posee para la empresa.

Seguidamente se presentan los datos que se consideran como activos dentro de la organización y que presentan una magnitud de daño mediano y alto. Ver (Anexo 10)

Tabla 3:

Activos en la categoría de datos con magnitud de daño mediano

N°	Activo	Clasificación		
		1	2	3
1	Base de datos internos	x		X
2	Base de datos externos	x		X
3	Infraestructura (planes, documentación)	x	x	X
4	Base de datos de contraseña	x	x	X

Tabla 4:

Activos en la categoría de datos con magnitud de daño alto.

N°	Activo	Clasificación		
		1	2	3
1	Proyectos institucionales (Proyectos, planes, evaluaciones, informes)	x	x	X
2	Finanzas	x		X
3	Servicios bancarios	x	x	X
4	Respaldos	x	x	X
	Datos e información no institucional	x		X

3.1.1.3.1.1.2 Sistemas

A continuación se muestran los activos que poseen riesgos en la categoría de sistemas. La escala de la magnitud del daño se calculó haciendo un análisis de los riesgos según tres clasificaciones:

Clasificación 1: Acceso exclusivo.

Clasificación 2: Acceso ilimitado.

Clasificación 3: Costo de recuperación (Tiempo, económico, material, imagen, emocional)

Seguidamente se presentan los sistemas que se consideran como activos dentro de la organización y que presentan una magnitud de daño mediano y alto. Ver (Anexo11)

Tabla 5:

Activos en la categoría de sistemas con magnitud de daño mediano.

N°	Activo	Clasificación		
		1	2	3
1	Equipos de red cableada (router, swich)	x		x
2	Equipos de la red inalámbrica (router, punto de acceso)	x		x
3	Programas de manejo de proyectos	x		x
4	Impresoras		x	x
5	PBX (Sistema de telefonía convencional)		x	x
6	Celulares		x	x
7	Edificio(Oficina, recepción, sala de espera, sala de reunión, bodega)		x	x
8	Vehículos		x	x

Tabla 6:

Activos en la categoría de sistemas con magnitud de daño alto

Nº	Activo	Clasificación		
		1	2	3
1	Cortafuegos	x		
2	Servidores	x		x
3	Computadoras		x	x
4	Portátiles		x	x
5	Programas de administración(contabilidad, manejo de personal)	x		x

3.1.2.3.1.1.3 Personal

A continuación se muestran los activos que poseen los riesgos en la categoría de personal. La escala de la magnitud del daño se calculó haciendo un análisis de los riesgos según tres clasificaciones:

Clasificación 1: Imagen pública de alto perfil, indispensable para funcionamiento institucional.
Clasificación 2: Perfil medio, experto en su área.
Clasificación 3: Perfil bajo, no indispensable para funcionamiento en su área.

Seguidamente se presentan los riesgos en la categoría de personal que se consideran como activos dentro de la organización y que presentan una magnitud de daño mediano y alto. Ver (Anexo 12)

Tabla 7:

Activos en la categoría de personal con magnitud de daño mediano

N°	Activo	Clasificación		
		1	2	3
1	Administración		x	
2	Personal Técnico		x	
3	Informática, soporte técnico interno		x	
4	Soporte técnico externo		x	

Tabla 8:

Activos en la categoría de personal con magnitud de daño alto

N°	Activo	Clasificación		
		1	2	3
1	Junta directiva	x		
2	Dirección coordinación	x		

3.1.1.3.2 Identificación de amenazas

Luego de haber identificado los activos de la empresa distribuidos por sus distintas categorías se procederá a la identificación de las amenazas distribuidas también por categorías que podrían incidir negativamente y afectar a los activos de la empresa.

En el presente trabajo se tendrán en cuenta las siguientes categorías de amenazas: Actos originados por la criminalidad común y motivación política,

sucesos de origen físico y sucesos derivados de la impericia, negligencias de usuarios y decisiones institucionales. Las mismas se encuentras distribuidas en las probabilidades de ocurrencia: Insignificante, baja, mediana y alta.

A continuación solo se presentarán las amenazas que se encuentran en la probabilidad de ocurrencia de mediana y alta por su importancia y riesgo que ocupa en el desarrollo de esta investigación.

3.1.1.3.2.1 Actos originados por la criminalidad común y motivación política

A continuación se detallan las amenazas relacionadas con los actos originados por la criminalidad común y motivación política.

Tabla 9:

Identificación de amenazas con probabilidad de ocurrencia mediana. Categoría actos originados por la criminalidad común y motivación política

Nº	Amenaza	Descripción
1	Fraude/Estafa	Dirigida a documentos de la empresa
2	Robo/Hurto Físico	Puede ser civil, fiscal o penal.
3	Robo/Hurto de información electrónica	Pude ser por trabajadores como por personas que no pertenecen a la empresa.
4	Intrusión a red interna	Daños por personas inescrupulosas que violentan la ley.
5	Infiltración	Dirigida hacia administrativos de alto rango.
6	Virus/ Ejecución no autorizada de programas	Cometida por miembros internos de la empresa.

En esta categoría no se presentan amenazas con probabilidad alta de ocurrencia.

3.1.1.3.2.2 Sucesos de origen físico

A continuación se representan las amenazas para la empresa en la categoría de los sucesos de origen físico con probabilidad de ocurrencia mediana y alta.

Tabla 10:

Identificación de amenazas con probabilidad de ocurrencia mediana. Categoría Sucesos de origen físico.

Nº	Amenaza	Descripción
1	Polvo	Alojado en el hardware de las computadoras originando fallas técnicas
2	Falla de sistema/daño disco duro	Falla electrónica

En esta categoría no se presentan amenazas con probabilidad alta de ocurrencia.

3.1.1.3.2.3 Sucesos derivados de la impericia/ negligencias de usuarios y decisiones institucionales

A continuación se detallan los sucesos derivados de la impericia y originados por la negligencia de los usuarios que pueden llegar a convertirse en amenazas para la empresa.

Tabla 11:

Definición de amenazas con probabilidad de ocurrencia mediana. Categoría Sucesos derivados de la impericia/ negligencias de usuarios y decisiones institucionales.

N°	Amenaza	Descripción
1	Falta de inducción, capacitación y sensibilización sobre riesgos.	Falta de preocupación por parte de los directivos
2	Mal manejo de sistemas y herramientas	Contrato de personal no capacitado para esta gestión.
3	Perdida de datos	Producido por fallas del sistema
4	Infección de sistemas a través de unidades portables sin escaneo	Unidades de almacenamiento de trabajadores de la empresa
5	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Irresponsabilidad del personal de la empresa
6	Exposición o extravío de equipo, unidades de almacenamiento.	Irresponsabilidad del personal de la empresa
7	Acceso electrónico no autorizado a sistemas internos.	Producido por personal no correspondiente a la empresa
8	Red cableada expuesta para el acceso no autorizado.	Infraestructura expuesta fuera de la empresa
9	Dependencia a servicio técnico externo	Contrato de personal no capacitado para esta gestión.

Tabla 12:

Definición de amenazas con probabilidad de ocurrencia alta. Categoría Sucesos derivados de la impericia/ negligencias de usuarios y decisiones institucionales

N°	Amenaza	Descripción
1	Compartir contraseñas o permisos a terceros no autorizados	Irresponsabilidad del personal de la empresa
2	Transmisión de contraseñas por teléfono	Irresponsabilidad del personal de la empresa
3	Red inalámbrica expuesta al acceso no autorizado	No implantar medidas de seguridad adecuada

3.1.1.3.3 Identificación de vulnerabilidades

Una vulnerabilidad en el sistema, es la incapacidad o debilidad demostrada para resistir una amenaza inminente y que al ocurrir afecta inevitablemente los activos de la empresa. Es la forma potencial de manifestación de la amenaza en el activo y su incidencia negativa.

Para identificar una vulnerabilidad se debe determinar la probabilidad de ocurrencia de la amenaza en cuestión.

Tabla 13:

Definición de frecuencias y probabilidad de ocurrencia de la amenaza

Frecuencia	Valor	Característica	Probabilidad de ocurrencia
Muy Frecuente	4	A diario	75 % - 100%(Alta)
Frecuente	3	Una vez x Mes	40% - 75%(Media)
Poco Frecuente	2	Una vez x Año	10% - 40%(Baja)
Raramente Frecuente	1	Prácticamente no ocurre	0 – 10% (Prácticamente no ocurre)

Las amenazas presentadas en el desarrollo de esta investigación fueron solamente las que su probabilidad de ocurrencia son mediana y alta, puesto que sus características son de suceder una vez al mes y a diario respectivamente y representan un mayor riesgo en la institución. Debido a esto todas estas amenazas extraídas constituyen vulnerabilidades para los activos de la empresa.

3.1.1.4 Identificación de impactos de los riesgos

Luego de tener lista la identificación de las amenazas que representan vulnerabilidades de la empresa, se procede como siguiente paso a la identificación de los posibles impactos de las amenazas en cada activo. Con el objetivo de agilizar el proceso solo se tendrán en cuenta aquellas relaciones activo-amenaza que son consideradas vulnerabilidades para aplicarles la magnitud del impacto.

Tabla 14:

Definición de la magnitud del impacto

Magnitud del impacto	Ponderación de la amenaza	Descripción
Alto	4	La vulnerabilidad o amenaza representa un problema serio para la organización.
Medio	3	La vulnerabilidad o amenaza debe ser tenido en cuenta cuando ocurra para mitigar sus efectos.
Bajo	2	La vulnerabilidad o amenaza no representa un alto riesgo, sin embargo debe prevenirse su ocurrencia.
Insignificante	1	La vulnerabilidad o amenaza no es relevante.

3.1.1.5 Identificar y evaluar opciones para el tratamiento de riesgos.

A partir de la información obtenida sobre la empresa Fideval, a través de la matriz establecida para determinar los riesgos sobre los activos de la misma, se realizó una gráfica que muestra el promedio aritmético de los diferentes riesgos, en relación con los diferentes grupos de amenazas y daños. La idea de esta figura es ilustrar, en qué grupo (combinación de Probabilidad de Amenaza y Magnitud de Daño) hay mayor o menor peligro, por lo que resultó ser el integrado por sistema-infraestructura junto a negligencia institucional, el cual posee un riesgo medio de 7,9. Ver (Anexo 13)

Otra de las gráficas generadas por la matriz es análisis de factores, quien tiene el mismo propósito que la hoja anterior con la diferencia que esta vez el promedio aritmético de los grupos está mostrado en un grafo, dependiendo de

la probabilidad de amenaza y magnitud de daño. La línea amarilla muestra el traspaso de la zona bajo riesgo a mediano riesgo y la línea roja, el traspaso de mediano riesgo a alto riesgo. Esta hoja ilustra el nivel de peligro por grupo y la influencia de cada factor por lo que se puede llegar a la misma conclusión que en la de la gráfica anterior. Ver (Anexo14)

Se identificarán como opciones para el tratamiento de los riesgos encontrados en esta matriz, la realización de un plan de seguridad que estará compuesto por un conjunto de medidas con el objetivo de mitigar todos los riesgos críticos capturados durante el proceso de investigación en la empresa.

En aquellos casos en los que se considere necesario, por criterios técnicos o reglamentarios se elaborarán informes de evaluación específicos que se incluirán como documentos anexos al documento de evaluación donde se describirán adicionalmente los riesgos encontrados en la empresa.

3.1.1.6 Seleccionar controles para el tratamiento de riesgos.

La seguridad de la información se divide en tres categorías que comúnmente se denominan controles:

- Físico
- Técnico
- Administrativo

Para mitigar los riesgos de alto impacto se establecen estos controles, los cuales ayudan a reducir el impacto y la probabilidad de ocurrencia de las amenazas que puedan ocasionar daños en la infraestructura de la institución.

Los controles a implementar están enfocados a los siguientes procesos:

3.1.1.6.1 Controles físicos

El control físico es la implementación de medidas de seguridad en una estructura definida usada para prevenir o detener el acceso no autorizado a material confidencial. Ejemplos de los controles físicos son:

- Establecer cámaras de circuito cerrado en la empresa
- Guardias de seguridad las 24 horas
- Identificación con fotos para la entrada de los trabajadores a la empresa
- Puertas de acero con seguros especiales.

3.1.1.6.2 Controles técnicos

Los controles técnicos utilizan la tecnología como una base para controlar el acceso y uso de datos confidenciales a través de una estructura física y sobre la red. Los controles técnicos son mucho más extensos en su ámbito e incluyen tecnologías tales como:

- Encriptación
- Autenticación a nivel de la red
- Control de acceso del personal a los activos de la empresa
- Instalación de software para medir la integridad de archivos por vía inalámbrica.

3.1.1.6.3 Controles administrativos

Los controles administrativos definen los factores humanos de la seguridad. Incluye todos los niveles del personal dentro de la organización y determina cuáles usuarios tienen acceso a qué recursos e información usando medios tales como:

- Entrenamiento y conocimiento del personal de la empresa.
- Planes de recuperación.
- Estrategias de selección de personal y separación
- Registro y contabilidad de personal

3.1.1.7 Obtener la aprobación de la gerencia para los riesgos residuales.

Los riesgos residuales son aquellos que permanecen después que la dirección de la entidad le da respuesta a los riesgos inherentes encontrados desarrollando acciones para corregirlos.

El proceso de prever estos riesgos es complicado, puesto que se espera que con la implantación del plan de medidas para mitigar los riesgos inicialmente encontrados, se obtengan buenos resultados y se erradiquen, pero al final cuando se implementan estas es que se conoce lo que realmente pasa con el sistema.

Antes de comenzar con el plan de medidas se le sugirió a la gerencia de la empresa Fideval que dieran la aprobación para en caso de que existieran riesgos residuales crear otro plan de seguridad con el fin de eliminarlos completamente de la empresa, lo cual fue aprobado.

3.1.1.8 Obtener la aprobación de la gerencia para la implementación de la norma ISO 27001.

Las empresas al implementar la norma de seguridad de la información ISO 27001 reciben ventajas comerciales como:

1. La empresa al implementar la norma cumple con los requerimientos legales, por lo que no viola ninguna ley sobre seguridad de la información.

2. Al concluir la implementación de la norma la empresa es certificada y quizás sus competidores no lo estén por lo que obtiene de esta forma una ventaja comercial ante los ojos de los clientes que les interesa tener de forma segura toda su información que en el caso de esta empresa tiene carácter monetario.

3. Evitando que se produzcan incidentes de seguridad se logra que la empresa se ahorre costos que serán mayores que el costo que supone la inversión en la norma ISO 27001.

4. La implementación de la norma ayuda a dejar en la empresa una mejor organización ya que alienta a las instituciones a describir sus principales procesos.

Al estar conscientes de este grupo de ventajas que se obtienen con la implementación de la norma ISO 27001, la gerencia de la empresa Fideval no sólo aprobó la implantación de la norma para la seguridad de su información, sino que añadió que era necesario para garantizar la continuidad y el éxito de la misma.

CAPÍTULO 4

GESTIÓN DE RIESGOS

4.1 IDENTIFICACIÓN DE RIESGOS

Luego de haber definido los activos y las amenazas a estos, identificado las vulnerabilidades y establecidos las magnitudes del impacto se procede entonces a la identificación de los riesgos. Para ello se propone la fórmula:

Riesgo Total (RT) = Magnitud del impacto * Probabilidad de ocurrencia

El riesgo, que es el producto de la multiplicación, magnitud del impacto y probabilidad de ocurrencia, está agrupado en tres rangos, y para su mejor visualización se aplican tres colores:

- Bajo riesgo: Ponderados en escala de 1 - 6 (Verde)
- Medio riesgo: Ponderados en escala de 8 - 9 (Amarillo)
- Alto riesgo: Ponderados en escala de 12 - 16 (Roja)

Se puede concluir entonces que solo se considerarán activos en riesgos altos aquellos cuya probabilidad de ocurrencia de las amenazas tengan un valor de mediano o alto y los activos presenten una magnitud impacto alto y viceversa.

Dependiendo del color de cada celda, se puede sacar conclusiones no solo del nivel de riesgo que corre cada elemento de información de sufrir un daño significativo, causado por una amenaza, sino también sobre las medidas de protección necesarias a implementar sobre la empresa.

4.1.1. Identificación de Riesgos Críticos

Como parte de la norma ISO 27001 es necesario para la empresa Fideval hacer una adecuada gestión de riesgos que le permita saber cuáles son los principales activos vulnerables, para en función de ello elaborar un plan de seguridad adecuado que mitigue los mismos y tener la tranquilidad que necesita. Para ellos es necesario ratificar que los activos que poseen riesgo alto serán los marcados en la matriz con la coloración roja y que la ponderación de la celda estará en el rango de 12-16. Ver (Anexo 1-9)

En la medida que la empresa tenga clara esta identificación de riesgos se podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

A continuación se representan los activos que poseen riesgo crítico:

- Documentos institucionales (Proyectos, planes, evaluaciones, informes, entre otros).
- Finanzas.
- Servicios bancarios.
- Base de datos interno.
- Base de datos externo.
- Respaldos.
- Infraestructura (Planes, Documentación)
- Base de datos con contraseñas.
- Datos e información no institucional.
- Cortafuegos.
- Servidores.
- Computadoras.
- Portátiles.

- Programas de administración (contabilidad, manejo de personal).
- Junta directiva.
- Dirección coordinación.
- Administración
- Personal Técnico
- Informática/Soporte técnico interno.
- Soporte técnico externo.

4.1.1.1 Clasificación de Riesgo Total

En base a la clasificación de los activos mostrados anteriormente se tendrá el tipo de riesgo a enfrentar. Los mismos se clasificarán en:

- Riesgo de integridad: Engloba todo lo referido al procesamiento de la información introducida a través de la interfaz de usuario y el aseguramiento que la misma sea trasmitida correctamente mediante las aplicaciones.
- Riesgo de acceso: Se concentra en el incorrecto acceso a los sistemas, datos e información referente a las empresas.
- Riesgo de utilidad: Engloba las técnicas de recuperación/restauración utilizadas para minimizar las rupturas del sistema y están contenidos los backups de información.
- Riesgo de infraestructura: Se refiere a que en las organizaciones no existe una infraestructura tecnológica adecuada para desarrollar las funciones en la organización.

4.1.1.2 Cálculo del Riesgo Residual (RR).

Como se había planteado anteriormente los riesgos residuales son aquellos que perduran después que la empresa intenta mitigar los riesgos inherentes encontrados tomando acciones para corregirlos.

Para el cálculo de este tipo de riesgo se utilizó la fórmula:

Riesgo Residual (RR) = RT – Salvaguarda

Salvaguarda = % protección * RT

Para calcular el por ciento de protección y consecutivamente la salvaguarda, se tuvo en cuenta los factores que influyen sobre cada riesgo definido anteriormente (riesgo de integridad, riesgo de acceso, riesgo de utilidad y riesgo de infraestructura). Los mismos se exponen a continuación:

- **Riesgo de Integridad**

1. Symantec EndPoint Protection: Antivirus que cubre el sistema en un 70%, protegiéndolo contra la entrada de hackers, realizando un filtrado de correos de la empresa y evitando un grupo de amenazas que afectan la seguridad de la institución.

2. Módulo Firewall: Módulo compuesto por un grupo de firewalls que cubre el sistema en un 80%, llevando el control de acceso de la red a nivel físico.

3. Bitácoras del uso de equipos y control de acceso: Se refiere al control sobre cada equipo de la empresa en cuanto a usuarios que han entrado al sistema, la fecha de mantenimiento de cada equipo, así como cualquier modificación realizada. Esto cubre el sistema en un 70%.

4. Políticas Active Directory: Se refiere a las políticas que se establecen en la empresa en cuanto a la administración de usuarios y sus inicios de sesión en cada equipo. Este servicio cubre el sistema en un 70%.

5. Políticas de departamento TI: Representa una importante herramienta conformada con un grupo de políticas que se establecen en las empresas, cuya utilidad es garantizar el buen funcionamiento de los procesos para optimizar los sistemas y garantizar la calidad en la gestión de las Tecnologías de la Información (TI), cubriendo el sistema en un 80%.

6. Manejo adecuado de equipos de cableado estructurado: El manejo adecuado de los equipos de cableado, que no es más que el tendido de cables de par trenzados en el interior de la empresa Fideval con el objetivo de establecer una red de área local. Ello garantiza la seguridad de la información que se trasmite mediante él, cubriendo el sistema en un 80%.

7. DLO Backups: Software que se ejecuta en computadoras de escritorio y portátiles y que garantiza la integridad de la información cubriendo el sistema en un 80%.

- **Riesgo de Acceso**

1. Políticas de uso de contraseña: Políticas dictadas por la empresa Fideval compuesta por una serie de medidas y buenas prácticas encaminadas a mejorar la seguridad de la institución en función de las contraseñas establecidas. Las mismas cubren el sistema en un 70%.
2. CheckPoint Firewall: Proveedor de soluciones de seguridad que cubre el sistema en cuanto a seguridad de red, seguridad de datos y gestión de seguridad. El mismo cubre el sistema en un 80%.

3. Políticas de acceso a File Server: Grupo de políticas que regula el control de acceso al servidor de archivos evitando una alteración del mismo en cuanto a la seguridad. Esto cubre el sistema en un 70%.
4. Mantenimiento preventivo y correctivo del hardware: Esto corrige los defectos o averías en el hardware de las computadoras preventivamente evitando la ruptura de la misma y garantizando el buen funcionamiento del sistema en un 60%.
5. Bitácoras de uso de equipos y control de acceso: Control de acceso sobre cada equipo en cuanto a lo realizado en el mismo por los usuarios, cubriendo el sistema en un 80%.
6. Symantec EndPoint Protection: Antivirus que cubre el sistema en un 80%, protegiendo el acceso ante terceras personas.

- **Riesgo de Utilidad**

1. Symantec EndPoint Protection: Antivirus que cubre el sistema en cuanto a las amenazas que ponen en riesgo de utilidad a los activos de la empresa Fideval en un 70%.
2. CheckPoint Firewall: Proveedor de soluciones de seguridad que cubre el sistema en cuanto a riesgos de utilidad en un 80%.
3. Políticas de departamento TI: Garantiza el buen funcionamiento del sistema en cuanto a seguridad, mantenimiento, respaldos de información y bitácoras creadas en función de las Tecnologías de la Información (TI), cubriendo el sistema en un 80%.

4. Políticas Active Directory: Este grupo de políticas cubre el sistema en un 70%.

5. Bitácoras de uso de equipos y control de acceso: Control de acceso sobre cada equipo de cómputo de la empresa, cubriendo el sistema en un 70%.

- **Riesgo de Infraestructura**

1. Symantec EndPoint Protection: Antivirus seleccionado por la empresa que cubre el sistema en un 70%.

2. Bitácoras de uso de equipos y control de acceso: Control de acceso sobre cada equipo de cómputo garantizando la infraestructura de la empresa, cubriendo el sistema en un 70%.

3. CheckPoint Firewall: Proveedor de soluciones de seguridad que cubre el sistema en cuanto a riesgos de infraestructura en un 80%.

4. Políticas Active Directory: Grupo de políticas nombradas por la empresa en cuanto a usuarios y sus respectivas sesiones, que cubre el sistema en un 70%.

5. Mantenimiento preventivo y correctivo del hardware: Prevee las averías del hardware de las computadoras de la empresa corrigiendo sus defectos, garantizando una buena infraestructura de la empresa y el buen funcionamiento del sistema en un 60%.

6. Políticas de departamento TI: Importante herramienta conformada con un grupo de políticas que se establecen en la empresa en cuanto a infraestructura de la misma, cuya utilidad es garantizar el buen funcionamiento de los procesos en cuanto a Tecnologías de la Información (TI), cubriendo el sistema en un 80%.

4.1.1.3 Cálculo del Riesgo Informático (RI)

Los riesgos informáticos no son más que los riesgos a los cuales están sometidos los procesos y actividades que participan en el área de la informática. Para calcular este riesgo se utilizó la fórmula:

Riesgo Informático (RI) = RR / RT

A continuación se muestran las amenazas que afectan los activos mencionados anteriormente, convirtiéndolos en activos con riesgo crítico, y el cálculo de su riesgo total atendiendo a la categoría del activo analizado, así como el riesgo residual y el riesgo informático. Los datos del cálculo del riesgo total fueron extraídos de la matriz de riesgo elaborada, constituida por los activos y sus amenazas pertenecientes a la empresa Fideval, la cual se encuentra en los anexos de la investigación. Ver (anexo 1-9).

Tabla 15:

Amenazas para el activo documentos institucionales y el cálculo de su riesgo

Amenazas	Cálculo del RT Integridad	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2

Tabla 16:

Amenazas para el activo documentos institucionales y el cálculo de su riesgo (Continuación)

Infección de sistemas a través de unidades portables sin escaneo	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de almacenamiento	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3

Tabla 17:

Amenazas para el activo documentos institucionales y el cálculo de su riesgo.

Amenazas	**Cálculo del RT Integridad**	**Cálculo del RR**	**Cálculo del RI**
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autorizado	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla18:

Amenazas para el activo finanzas y el cálculo de su riesgo

Amenazas	Cálculo del RT de Utilidad	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2

Tabla 19:

Amenazas para el activo finanzas y el cálculo de su riesgo

Amenazas	**Cálculo del RT de Utilidad**	**Cálculo del RR**	**Cálculo del RI**
Infección de sistemas a través de unidades portables sin escaneo	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de almacenamiento, entre otros.	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 20:

Amenazas para el activo servicios bancarios y el cálculo de su riesgo

Amenazas	Cálculo del RT de Infraestructura	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2
Infección de sistemas a través de unidades portables sin escaneo	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3

Tabla 21:

Amenazas para el activo servicios bancarios y el cálculo de su riesgo (Continuación)

Exposición o extravío de equipo, unidades de almacenamiento, entre otros.	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 22:

Amenazas para el activo Bases de datos internos y el cálculo de su riesgo

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Compartir contraseñas o permisos a terceros no autorizado	12	3.6	0.3
Transmisión de contraseñas por teléfono	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	12	3.6	0.3

Tabla 23:

Amenazas para el activo Bases de datos externas y el cálculo de su riesgo

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Compartir contraseñas o permisos a terceros no autorizado	12	3.6	0.3
Transmisión de contraseñas por teléfono	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	12	3.6	0.3

Tabla 24:

Amenazas para el activo Respaldos y el cálculo de su riesgo

Amenazas	Cálculo del RT de Utilidad	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3

Tabla 25:

Amenazas para el activo Respaldos y el cálculo de su riesgo (Continuación)

Amenazas	Cálculo del RT de Utilidad	Cálculo del RR	Cálculo del RI
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2
Infección de sistemas a través de unidades s/scan	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de almacenamiento	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 26:

Amenazas para el activo Infraestructura (Planes, Documentación) y el cálculo de su riesgo

Amenazas	Cálculo del RT de Infraestructura	Cálculo del RR	Cálculo del RR
Compartir contraseñas o permisos a terceros no autorizado	12	3.6	0.3
Transmisión de contraseñas por teléfono	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	12	3.6	0.3

Tabla 27:

Amenazas para el activo Base de datos con contraseñas y el cálculo de su riesgo

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Compartir contraseñas o permisos a terceros no autorizado	12	3.6	0.3
Transmisión de contraseñas por teléfono	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	12	3.6	0.3

Tabla 28:

Amenazas para el activo Datos e información no institucionales y el cálculo de su riesgo

Amenazas	Cálculo del RT de Integridad	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3

Tabla 29:

Amenazas para el activo Datos e información no institucionales y el cálculo de su riesgo (Continuación)

Amenazas	Cálculo del RT de Integridad	Cálculo del RR	Cálculo del RI
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2
Infección de sistemas a través de unidades portables	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de almacenamiento	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 30:

Amenazas para el activo Cortafuego y el cálculo de su riesgo

Amenazas	Cálculo de RT de Acceso	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2
Infección de sistemas a través de unidades portables sin escaneo	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de almacenamiento.	12	3.6	0.3

Tabla 31:

Amenazas para el activo Cortafuego y el cálculo de su riesgo (Continuación)

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 32:

Amenazas para el activo Servidores y el cálculo de su riesgo

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Perdida de datos	12	2.4	0.2

Tabla 33:

Amenazas para el activo Servidores y el cálculo de su riesgo (Continuación)

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Infección de sistemas a través de unidades portables sin escaneo	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de almacenamiento.	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 34:

Amenazas para el activo Computadoras y el cálculo de su riesgo

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2

Tabla 35:

Amenazas para el activo Computadoras y el cálculo de su riesgo (Continuación)

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2
Infección de sistemas a través de unidades portables sin escaneo	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de almacenamiento.	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 36:

Amenazas para el activo Portátiles y el cálculo de su riesgo

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2
Infección de sistemas a través de unidades portables sin escaneo	12	3.6	0.3
Manejo inadecuado de contraseñas	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de almacenamiento.	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3

Tabla 37:

Amenazas para el activo Portátiles y el cálculo de su riesgo (Continuación)

Amenazas	Cálculo del RT de Acceso	Cálculo del RR	Cálculo del RI
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 38:

Amenazas para el activo Programas de administración (contabilidad, manejo de personal) y el cálculo de su riesgo.

Amenazas	Cálculo de RT de Utilidad	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2

Tabla 39:

Amenazas para el activo Programas de administración (contabilidad, manejo de personal) y el cálculo de su riesgo (Continuación)

Amenazas	Cálculo de RT de Utilidad	Cálculo del RR	Cálculo del RI
Perdida de datos	12	2.4	0.2
Infección de sistemas a través de unidades portables sin escaneo	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de almacenamiento.	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 40:

Amenazas para el activo Junta directiva y el cálculo de su riesgo

Amenazas	Cálculo del RT Infraestructura	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2
Infección de sistemas a través de unidades portables sin escaneo	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3

Tabla 41:

Amenazas para el activo Junta directiva y el cálculo de su riesgo (Continuación)

Amenazas	Cálculo del RT Infraestructura	Cálculo del RR	Cálculo del RI
Exposición o extravío de equipo, unidades de almacenamiento, entre otros	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 42:

Amenazas para el activo Dirección/coordinación y el cálculo de su riesgo

Amenazas	Cálculo del RT Infraestructura	Cálculo del RR	Cálculo del RI
Fraude / Estafa	12	3.6	0.3
Robo / Hurto (físico)	12	3.6	0.3
Robo / Hurto de información electrónica	12	3.6	0.3
Intrusión a Red interna	12	2.4	0.2

Tabla 43:

Amenazas para el activo Dirección/coordinación y el cálculo de su riesgo (Continuación)

Amenazas	Cálculo del RT Infraestructura	Cálculo del RR	Cálculo del RI
Infiltración	12	2.4	0.2
Virus / Ejecución no autorizado de programas	12	3.6	0.3
Polvo	12	4.8	0.4
Falla de sistema / Daño disco duro	12	2.4	0.2
Falta de inducción, capacitación y sensibilización sobre riesgos	12	2.4	0.2
Mal manejo de sistemas y herramientas	12	2.4	0.2
Perdida de datos	12	2.4	0.2
Infección de sistemas a través de unidades portables	12	3.6	0.3
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	12	3.6	0.3
Compartir contraseñas o permisos a terceros no autorizado	16	4.8	0.3
Transmisión de contraseñas por teléfono	16	4.8	0.3
Exposición o extravío de equipo, unidades de cd	12	3.6	0.3
Acceso electrónico no autorizado a sistemas internos	12	3.6	0.3
Red cableada expuesta para el acceso no autorizado	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	16	3.2	0.2
Dependencia a servicio técnico externo	12	2.4	0.2

Tabla 44:

Amenazas para el activo Administración y el cálculo de su riesgo

Amenazas	Cálculo del RT Infraestructura	Cálculo del RR	Cálculo del RI
Compartir contraseñas o permisos a terceros no autorizado	12	3.6	0.3
Transmisión de contraseñas por teléfono	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	12	3.6	0.3

Tabla 45:

Amenazas para el activo personal técnico y el cálculo de su riesgo

Amenazas	Cálculo del RT Infraestructura	Cálculo del RR	Cálculo del RI
Compartir contraseñas o permisos a terceros no autorizado	12	3.6	0.3
Transmisión de contraseñas por teléfono	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	12	3.6	0.3

Tabla 46:

Amenazas para el activo Informática/Soporte técnico interno y el cálculo de su riesgo

Amenazas	Cálculo del RT Infraestructura	Cálculo del RR	Cálculo del RI
Compartir contraseñas o permisos a terceros n/aut.	12	3.6	0.3
Transmisión de contraseñas por teléfono	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	12	3.6	0.3

Tabla 47:

Amenazas para el activo Informática/Soporte técnico interno y el cálculo de su riesgo

Amenazas	Cálculo del RT Infraestructura	Cálculo del RR	Cálculo del RI
Compartir contraseñas o permisos a terceros no autorizado	12	3.6	0.3
Transmisión de contraseñas por teléfono	12	3.6	0.3
Red inalámbrica expuesta al acceso no autor	12	3.6	0.3

4.1.2 Consecuencias de las amenazas sobre cada activo con riesgo crítico en la empresa Fideval.

Haciendo un estudio de las principales amenazas que significaron un mayor riesgo sobre los activos de la empresa Fideval, se llegó a la conclusión que fueron las que correspondían a la ponderación con el número 16 al realizar el cálculo del riesgo . Las mismas se nombran a continuación:

- Compartir contraseñas o permisos a terceros no autorizados.
- Transmisión de contraseñas por teléfono.
- Red inalámbrica expuesta al acceso no autorizado

A continuación se hará una explicación detallada de estas principales amenazas sobre los activos de la empresa y sus consecuencias.

4.1.2.1 Consecuencias de las amenazas detectadas sobre el activo Documentos institucionales

Un documento institucional es aquel en el cual se establecen los objetivos del centro donde es emitido, facilitan la información, la comunicación y la coordinación de acciones que se realizan dentro de la institución evitando así la improvisación y realizan procesos de evaluación interna promoviendo propuestas de mejora.

La empresa Fideval cuenta con varios documentos institucionales que rigen las principales funciones de la institución y constituyen por tanto una fuente de datos vulnerables que solo debe estar en manos de los trabajadores de la misma.

El hecho de que se comparta las contraseñas o permisos de las computadoras de la empresa a terceros no autorizados pone en riesgo la fidelidad de estos documentos y por ende la seguridad de la empresa.

Transmitir contraseñas de informes de gran importancia por vías no seguras como son las telefónicas pone en riesgo que estas queden en mano de personas que las utilicen con otros fines y que además sean modificadas, lo que pone en peligro la empresa puesto que cuando estos documentos vayan a ser utilizados no se encuentran en el estado inicial.

Lo mismo pasa con la intromisión de agentes externos a la empresa por vía inalámbrica lo que constituye un riesgo al poner en sus manos documentos institucionales que solo pueden ser utilizados por parte de los trabajadores de la empresa.

4.1.2.2 Consecuencias de las amenazas detectadas sobre el activo finanzas

Las finanzas de una empresa están divididas en dos funciones principales: la función de inversión y la función de financiamiento. En esta área se establecen todos los datos de índole monetario en cuanto a inversiones que realiza y realizará la empresa y el dinero con que se dispone para ejecutar estas funciones.

El hecho de que se compartan contraseñas a terceros no autorizados por la empresa, se transmitan contraseñas por vías no seguras como las telefónicas y puedan existir intrusos por red inalámbrica pone en riesgo a la empresa en cuanto a que este personal ajeno a la institución cuente con la cifra exacta del capital con que dispone la empresa para realizar inversiones de su naturaleza por tanto esto constituye un riego alto en la misma.

4.1.2.3 Consecuencias de las amenazas detectadas sobre el activo servicios bancarios

Un excelente servicio al cliente puede mejorar la capacidad del banco de atraer a clientes potenciales ricos, elevar la rentabilidad del mismo, así como disminuir sus costos de operación, y/o crear una mayor lealtad de los clientes.

Los bancos son empresas donde los datos poseen carácter monetario, o sea poner en manos de terceras personas estos datos puede significar la pérdida de un gran volumen de dinero y con ello consecuencias de carácter crítico para la entidad.

La protección de datos es un tema cada vez más fundamental en la estrategia empresarial para mantener la continuidad del negocio y la clave para una protección efectiva es la encriptación o cifrado de los datos más sensibles.

Al mismo tiempo que aumenta el volumen de datos en tránsito por vías no seguras se incrementa la responsabilidad de las empresas por mantener la privacidad de los datos que manejan, lejos del alcance de la cyber-delincuencia y de prácticas malintencionadas. A esa creciente exigencia se une la obligatoriedad de cumplimiento de las regulaciones en materia de protección de datos.

Tras una estrategia de protección de datos está en juego la reputación y la continuidad de la empresa, es por ello que se debe tener total cuidado con amenazas para la empresa como son compartir contraseñas a terceros no autorizados por la empresa, la transmisión de contraseñas de la institución por vías no seguras como las telefónicas y el hecho de que puedan existir intrusos por red inalámbrica, para de esta manera estar seguros de dar a los clientes la seguridad y privacidad necesarias para su fidelización, y por ende la buena salud del negocio en cuestión de servicios bancarios.

4.1.2.4 Consecuencias de las amenazas detectadas sobre el activo Respaldos

Backup o respaldos es el procedimiento utilizado para hacer copias de información. Estas copias de seguridad se deben realizar sobre los datos más importantes con el propósito que estén disponibles en caso de fallas de nuestros sistemas.

De otra manera se puede decir que un backups de información es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma

más económica que los discos duros y además permitir de alguna forma el traslado a ubicaciones distintas de la de los datos originales.

La mayoría de las empresas son conscientes que en cualquier momento los sistemas pueden ser invadidos por intrusos y en general realizan sus copias de información, pero pasan por alto algunos aspectos importantes que se deben tener en o copias de cuenta al realizar un Backup seguridad como lo es que esos datos deben permanecer de una manera segura ya que puede existir infiltraciones en la información.

La empresa Fideval cuenta con una gran cantidad de información debido a los servicios que presta la misma, es por ello que se vuelve un riesgo poseer esta información sin tomar las medidas pertinentes de precaución en caso de que hubiese infiltraciones en la misma emitidas por red inalámbrica, por compartir contraseñas o permisos a terceros no autorizados o por la transmisión de contraseñas por vía telefónica.

Debido a esto se debe poner las medidas técnicas necesarias en la empresa para preservar los sistemas adecuadamente protegiendo en gran medida los backups de información ya que una pérdida de esta información vulnerable puede suponer altísimos costes para esta organización.

4.1.2.5 Consecuencias de las amenazas detectadas sobre el activo Datos e información no institucional

La información no institucional es aquella que la empresa posee en sus manos para realizar cualquier actividad propia y que se hace necesario tenerla, pero que no le pertenece.

El manejo inadecuado de sus datos resulta un riesgo puesto que en manos de la institución están informaciones vulnerables de otras empresas que al darle un manejo inadecuado pueden resultar perjudicadas de muchas maneras.

Es por ello que se debe tener especial atención a que estos datos estén en extremo cuidados y que los mismos no se encuentren amenazados con que de alguna vía puedan estar en manos de personas no autorizadas por la empresa puesto que esto resultaría un gran peligro para ella y para la empresa comprometida.

4.1.2.6 Consecuencias de las amenazas detectadas sobre el activo Cortafuego

El cortafuego está diseñado para dos funciones específicamente: bloquear el acceso no autorizado y permitir comunicaciones autorizadas con la computadora sobre la base de un conjunto de reglas.

Este sistema es utilizado en la empresa Fideval para evitar que los usuarios no autorizados tengan acceso a su red privada, por tanto todos los mensajes que entren o salgan de la empresa pasan a través del mismo para examinarlos y de esta manera bloquea aquellos que no cumplan con los criterios de seguridad establecidos por la institución.

El hecho de que su contraseña esté en manos de personas no autorizadas o ajenas a la entidad pone en peligro la seguridad de la empresa y con ellos la seguridad de su información, es por ello que es de vital importancia su conservación.

4.1.2.7 Consecuencias de las amenazas detectadas sobre el activo Servidores

El servidor es un ordenador cuyo propósito es proveer datos a un grupo de máquinas en red. Estos dispositivos poseen gran calidad de procesamiento pues están constituidos para servir información necesaria todo el tiempo.
Cuando algún usuario se conecta a un servidor pueden acceder a archivos, programas e informaciones que se encuentran en él de todo tipo.
La empresa Fideval cuenta con varios servidores donde se almacena información confidencial de la institución. Es por ello que se debe tomar medidas en cuanto a la intención de terceras personas por entrar a estas máquinas servidoras y tomar información que puede ser vulnerable para la empresa por vías solamente autorizadas para el personal de la misma.

4.1.2.8 Consecuencias de las amenazas detectadas sobre el activo Computadoras- Portátiles

A través del uso de los ordenadores se logran importantes mejoras en la empresa, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y lo más importante, su implantación logra ventajas competitivas o reducir la ventaja de los rivales.

La información se ha colocado en un buen lugar como uno de los principales recursos que poseen las empresas actualmente. Los entes que se encargan de las tomas de decisiones han comenzado a comprender que la información no es sólo un subproducto de la conducción empresarial, sino que a la vez alimenta a los negocios y puede ser uno de los tantos factores críticos para la determinación del éxito o fracaso de éstos.

Si se desea maximizar la utilidad que posee la información, el negocio la debe manejar de forma correcta y eficiente, tal y cómo se manejan los demás recursos existentes. Los administradores deben comprender de manera general

que hay costos asociados con la producción, distribución, seguridad, almacenamiento y recuperación de toda la información que es manejada en la organización.

El robo de información sensible y secretos corporativos es uno de los delitos con mayor incidencia en las empresas no solo a nivel mundial, sino también en Ecuador.

Es por ello que se debe tener mucho cuidado con los ordenadores de las empresas, porque ellas al contener información importante constituyen un activo de mucha relevancia dentro de la entidad y en base a esto se deben plantear las medidas pertinentes para evitar el robo de la información que contienen las mismas.

4.1.2.9 Consecuencias de las amenazas detectadas sobre el activo Programas de administración (contabilidad, manejo de personal)

Existen programas dentro de la empresa que constituyen la esencia en cuanto a la producción de la misma y por ende fuentes necesarias para su correcto funcionamiento. Tal es el caso de los programas de administración quienes en su interior llevan consigo todas las políticas administrativas que se desempeñan en la empresa.

En caso de que se puede acceder a alguno de estos programas de administración en la empresa Fideval por alguna vía de las amenazas expuestas anteriormente tendrán consigo descripciones administrativas lo que resulta información vulnerable para la empresa.

4.1.2.10 Consecuencias de las amenazas detectadas sobre el activo Junta directiva.

La junta directiva está formada por los principales dirigentes de una empresa donde se toman decisiones importantes dentro de la misma y se realizan actas de los acuerdos emitidos en forma digital. Esta junta directiva es elegida por los accionistas de la empresa pues en misma está en manos el futuro de la misma.

Estas actas que se realizan en estas reuniones quedan dentro de computadoras del trabajador que la confeccionó, por lo que resulta necesario que la misma tenga las medidas de seguridad pertinentes puesto que si alguna de estas llega a ser tomada por alguna persona ajena a la entidad causaría grandes problemas en cuanto a que estaría en sus manos decisiones posteriores que tomará la empresa en cuanto a aspectos de su interés.

4.1.2.11 Consecuencias de las amenazas detectadas sobre el activo Dirección/coordinación

La dirección de una empresa no es una tarea fácil. La misma persigue la satisfacción de los objetivos institucionales por medio de una estructura determinada y a través del esfuerzo humano coordinado.

Para dirigir una empresa es necesario contar con un grupo de trabajadores dentro de la organización que responden a la realización de todo un grupo de actividades, de las cuales algunas son ejecutadas con información vulnerable, lo que requiere de la imposición de contraseñas para acceder a estos datos, que deben ser otorgadas y coordinadas por la dirección de la institución en manos de quien deben estar.

La dirección de la empresa debe tener el control de las personas que entran a estos sistemas con contraseña y de qué trabajador es la responsabilidad para en base a esto tomar las medidas pertinentes.

4.2 CÁLCULO DEL RIESGO INFORMÁTICO

Para realizar el cálculo del riesgo informático de esta investigación es necesario calcular antes el riesgo total y el riesgo residual.

RT = RT integridad + RT acceso + RT utilidad + RT Infraestructura

RT= 504 + 1116 + 756 + 936

RT = 3312

RR = RR integridad + RR acceso + RR utilidad + RR Infraestructura

RR = 133.6 + 299.6 + 200.4 + 254.4

RR = 888

RI = RR / RT

RI = 888 / 3312

RI = 0.27

RI = 27%

El riesgo informático calculado es de un 27%, lo que significa que la empresa Fideval debe implementar medidas de protección basadas en los resultados de los activos identificados con riesgo para mitigar los mismos. Para que las medidas sean exitosas es necesario que siempre se verifique que sea las más factibles, es decir que técnicamente cumplan su propósito y funcionen con el respaldo y la aprobación para su implantación de la dirección de la

empresa Fideval. Además deben estar diseñadas de forma tal que no paralicen los procesos de la institución sino que ayuden a su mejor funcionamiento.

4.3. PLAN DE SEGURIDAD

La información es hoy en día uno de los activos más importantes con los que cuenta cualquier empresa; un activo que no siempre tiene la consideración e importancia necesaria dentro de algunas de estas entidades.

Antiguamente toda la información era almacenada en papel, por lo que toda su seguridad se limitaba a una seguridad física, actualmente existen multitud de dispositivos en los que se puede almacenar la información, por lo tanto la forma de evitar accesos a esa información es diferente.

Actualmente la naturaleza y la forma de difusión de los ataques ha cambiado; antes los hackers buscaban producir daños en los sistemas por el simple hecho de conseguir un poco de fama, actualmente sólo buscan obtener información y dinero levantando el menor revuelo posible y siempre aprovechando los recursos disponibles en la Web.

Es necesario hacer ver a las empresas la importancia que tiene la seguridad de su información dentro de sus procesos de negocio puesto que una pérdida de información puede comprometer negocios que en algunos casos podrían llegar a suponer pérdidas millonarias para las empresas.

Las grandes empresas (varias sucursales y mucho personal) suelen ser muy sensibles al aplicar técnicas de seguridad informática en su organización puesto que en general son conscientes del peligro que supone tener su red interna y sus equipos, al estar abiertos al exterior, o a un posible ataque interno. Sin embargo en el caso de empresas pequeñas (pequeñas sucursales y poco personal) la seguridad informática no suele ser un tema de máxima prioridad

por lo que pueden llegar a tener problemas de pérdidas de información o de intrusismos en su red.

Por ello es necesario poner énfasis en esas medianas y pequeñas empresas para conseguir hacer ver a sus responsables que los datos de su negocio pueden verse comprometidos intencionada o accidentalmente en cualquier momento y sin que ellos puedan hacer nada para remediarlo si no disponen de un correcto sistema de seguridad y respaldo.

Las organizaciones necesitan (en ocasiones deben) demostrar que realizan una gestión competente y efectiva de la seguridad de los recursos y datos que gestionan, pues deben demostrar que identifican y detectan los riesgos a los que está sometida y que adoptan medidas adecuadas y proporcionadas para que sus clientes tengan la seguridad que cuentan con empresas seguras.

A nivel mundial existen muchos estándares de seguridad de la información que ayudan a la misma a mitigar los riesgos a los que se enfrenta.

Por la importancia que se le concede a este tema, en esta investigación se utilizó el estándar de seguridad de la información ISO 27001 para gestionar los riesgos informáticos de la empresa Fideval y en base a ello realizar un plan de seguridad para mitigar todos los riesgos encontrados en la misma.

Una vez que se ha detectado una amenaza, real, imaginaria, probable o no, y se ha decidido hacer un plan para enfrentarse a ella, se debe analizar la situación y determinar los elementos que son relevantes, observando las relaciones entre ellos y la forma que tenemos de influir sobre los mismos.

Después de detectadas estas amenazas sobre los activos de la empresa se analizan y se extraen de las mismas los riesgos los cuales se clasifican en riesgo de nivel bajo, medio y alto. Seguido de esto se realiza un plan de

seguridad para mitigar los mismos los cuales solo ponen en constante peligro a la empresa.

Descrito así, el modelo de toma de decisiones puede aplicarse a cualquier situación en la que hagamos un plan para afrontarla y no solamente a las situaciones amenazantes o problemáticas sino también a toda aquella que al menos signifique un poco de peligro para la entidad.

4.3.1. Programas de Seguridad

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. El riesgo informático encontrado en esta investigación es de un 27% por lo que se hace imprescindible definir programas que garanticen la seguridad de la empresa Fideval.

Muchos son los softwares realizados en función de la seguridad de las empresas en diferentes áreas, a continuación se citan algunos de ellos:

- **Antivirus**

Los antivirus son programas especialmente diseñados para detectar y eliminar todo tipo de malwares como virus, troyanos, gusanos, rootkits, keyloggers. Actualmente algunos de ellos tienen potentes suites de seguridad añadidos como: antispywares, antispam, firewalls, antirootkit, navegación web segura.

Ejemplos de los mejores antivirus:

Symantec EndPoint Protection v12: Antivirus que ofrece seguridad inmejorable, rendimiento deslumbrante y una administración más inteligente en entornos físicos y virtuales. Mediante la red de inteligencia global más grande del mundo, Symantec puede identificar archivos en riesgo y detener las amenazas de día cero sin ralentizar el rendimiento. Se puede decir además que el mismo brinda la seguridad y protección más efectiva y rápida disponible.

Su vía de funcionamiento es analizar las características de los archivos sospechosos para determinar si ponen en riesgo sus sistemas. Promete una administración inteligente y ofrece protección en capas para Windows, Mac, Linux y máquinas virtuales.

Malwarebytes Anti-Malware 2.0.3.1025: Busca software dañino con opción a eliminarlos. Puede programarse para analizar el ordenador a una hora determinada. Cuenta además con una lista para ficheros en cuarentena y a ignorar. Existe la posibilidad de activar la protección en tiempo Real (detecta las amenazas antes que ingresen al sistema).

SpywareBlaster 5.0: Previene la ejecución de virus, de este modo bloquea totalmente su entrada previniendo acciones potencialmente peligrosas. Este se encargará de mantener actualizada su lista de virus peligrosos a través de Internet y tapar las posibles entradas maliciosas. Además permitirá realizar una captura del sistema para restaurarlo el algún momento.

SuperAntiSpyware 6.0.1170: Busca software dañino con opción a eliminarlos. Puede programarse para analizar el ordenador a una hora determinada. Cuenta además con una lista para ficheros en cuarentena y a

ignorar. Existe la posibilidad de activar la protección en tiempo Real (detecta amenazas antes que ingresen al sistema).

- **Firewall o Cortafuegos**

Es un mecanismo de seguridad contra ataques de Internet. Filtra y controla todas las comunicaciones que pasan de una red a otra evitando el ingreso y salida de ciertos procesos o aplicaciones.

Ejemplo de cortafuegos:

CheckPoint: Cortafuegos que se especializada en soluciones de seguridad lógica, cubriendo desde usuarios finales hasta proveedores de servicios de Internet. Esta tecnología está pensada para protegerse contra ataques y detectarlos de manera rápida y efectiva para proteger las entidades ofreciendo un nivel elevado de seguridad.

Ashampoo Firewall 1.20: Herramienta ideal para aquellos usuarios que se están iniciando en este tipo de aplicaciones. Constituye un intuitivo cortafuegos, fácil de usar y potente al mismo tiempo. Se caracteriza por poseer una sencilla interfaz.

Outpost Security Suite Free 7.1.1: Efectivo firewall que protege la privacidad, información y acceso a su ordenador sin el consentimiento. Dentro de sus principales características están la detección de intrusos, filtros, vigilancia del correo electrónico, bloqueo antispam, control de privacidad y licencia gratuita.

PC Tools Firewall Plus 7.0.0.123: Programa simple de usar que impide que se acceda a una PC desde el exterior. Dispone de las funciones como la

configuración de reglas avanzadas y zonas de confianza para direcciones, puertos y aplicaciones o el registro en tiempo real de la actividad de la red, todo esto sin un consumo excesivo de recursos.

- **Anti-Spam**

Se llama spam o correo basura a los mensajes de correo no solicitados, no deseados o de remitente desconocido, y que son muy molestosos.

Ejemplo de Anti-spam:

Symantec Brightmail: Hace que el correo electrónico sea más seguro y productivo y ofrece a las empresas defensas contra amenazas y span de tipo avanzado. Este programa identifica los mensajes que no son legítimos los cuales ocasionan la pérdida de oportunidades de negocio y de productividad del usuario final, y gracias a su uso, los usuarios no pasan por alto los mensajes importantes de correo electrónico.

Mailwasher Free 7.3: Este programa comprueba y administra los e-mails que se recibe, permitiendo eliminarlos sin necesidad de descargar los que no desee. Esta es una de las mejores medidas para evitar spam indeseado cuando ya ha llegado al correo del cliente.

SPAMfighter Pro 7.6.82: Es un filtro completo y fácil de usar que se añade a Outlook y Oulook Express, ayudándo en la tarea de eliminación de cualquier correo no deseado. Al adjuntarse en el propio cliente de correo de Microsoft sólo será necesario configurarlo, momento en el que se puede ver la facilidad

de uso y claridad de opciones disponibles. Incluye una lista negra y una lista de aceptados.

Spamihilator 1.5: Se trata de un filtro que actúa entre cliente - servidor, examinando cada uno de los mensajes que se descarga y dejando pasar sólo aquellos que cumplan ciertas normas.

- **Anti-Rootkits**

Como se ha explicado en la sección conceptos, un Rootkit es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers con el objetivo de acceder ilícitamente a un sistema informático.

Ejemplo de Anti-Rootkits:

Kaspersky TDSSKiller 2.8.16: Herramienta gratuita para eliminar los peligrosos rootkit de la familia Rootkit.Win32.TDSS: Tidserv, TDSServ y Alureon. Se trata de virus muy difíciles de detectar y eliminar con antivirus tradicionales. Al finalizar, el escaneo marcará los archivos sospechosos en amarillo y los peligrosos en rojo.

RegRun Reanimator 6.9.7.124: Completa suite de seguridad diseñada para detectar y eliminar virus, troyanos, spyware e incluso los nuevos y resistentes rootkits. Esta suite no es un buen complemento que incluye más de una treintena de funciones/utilidades para 'vigilar' a fondo tu sistema; optimizar el inicio, capturar rootkits, proteger los archivos del sistema, monitorizar las conexiones a Internet, entre otros.

Sophos Anti-Rootkit 1.5.2: Sencilla herramienta es capaz de localizar y eliminar cualquier rootkit que se haya escondido en tu sistema, analizando para ello todas tus unidades de disco, procesos activos y Registro de Windows.

- **Utilitarios Informáticos**

Los Utilitarios informáticos permiten optimizar nuestros sistemas operativos, navegadores, discos, haciéndolos más rápidos y eficientes. En ocasiones extremas, cuando los utilitarios no parecen arreglar la velocidad o funcionamiento del sistema, es cuando ya se necesita formatear.

Ejemplo de utilitarios informáticos:

CCleaner 4.13.4693: Herramienta que ayuda a mantener un sistema en buen estado, haciendo una limpieza a fondo que contribuye a mejorar el rendimiento general y aumentar el espacio libre en disco. Elimina archivos temporales, que no se usan o que quedan después de instalaciones o desinstalaciones y listas de ficheros usados recientemente, además de vaciar la papelera y eliminar los rastros de navegación como cookies, memoria caché, archivos temporales de Internet, direcciones web.

System Mechanic Free 12: Nos permite buscar, eliminar archivos duplicados y obsoletos, eliminar los rastros de navegación por Internet, arreglar entradas en el registro no válidas, optimizar el menú Inicio de Windows, protege la página de inicio y los programas que cargan al arrancar el sistema operativo, posee un limpiador de archivos innecesarios, desinstalador de aplicaciones, acelerador de Internet y de unidades de disco, gestor avanzado de procesos, entre otros.

Super Utilities Pro 9.9.8.8: Esta colección de herramientas permitirá optimizar, proteger y poner a punto el sistema, además de mejorar sensiblemente su velocidad y rendimiento general. Incluye limpieza de ficheros, disco, registro y otras herramientas que además vienen presentadas en una interfaz agradable y sencillo.

- **Programas de bloqueo y restricción**

Son programas realizados para bloquear y restringir el acceso a archivos, carpetas y discos duros de la computadora desde un lugar fuera de la entidad.

Ejemplo de programas de bloqueo y restricción:

Free Hide Folder 2.6: Es un programa que permite ocultar las carpetas privadas, de tal forma personas extrañas no podrán acceder a la información personal de una empresa.

My Lockbox 3.0: Permite tener una carpeta oculta y protegida con contraseña de manera fácil y rápida.

Folder Lock 7.2.2: Oculta ficheros confidenciales. Puede proteger con contraseñas, bloquear, esconder y encriptar cualquier número de archivos, carpetas, unidades, imágenes y documentos en segundos. La protección trabaja aún si los archivos son llevados de una computadora a otra en un disco removible, sin la necesidad de instalar ningún software.

- **Programas para copias de seguridad**

Programas que permiten realizar copias de seguridad de los principales archivos de un ordenador. Es importante hacer un backup permanente de nuestros archivos personales. También puede hacer una copia de seguridad manual en CD, DVD, USB, Discos Duros u otras Particiones.

Ejemplo de programas para copias de seguridad:

Symantec DLO (Usuario): Este programa ofrece copias de seguridad y recuperación de archivos automatizadas y confiables para equipos de escritorio y portátiles, proporcionando protección de datos de manera continua. Se puede decir además que el mismo cuenta con un mecanismo de reparación que

verifica de manera rápida la integridad de los datos duplicados y toma medidas correctivas, lo que le brinda una mayor confiabilidad y control de las copias de seguridad de datos.

HP Data Protector (Servidores): Software que ayuda a cumplir con los desafíos actuales y futuros de copia de seguridad y recuperación, y con los requisitos de la empresa, con una arquitectura sólida diseñada para ampliarse desde pequeñas y medianas empresas, a los entornos de tecnologías más complejos y más grandes del mundo. La solución mejora la continuidad empresarial y la capacidad de recuperación de datos y es muy utilizado en los servidores funcionando de manera óptima y potente

Cobian Backup 11.2.0.582: Es un programa creador y gestor de copias de seguridad. Permite gestionar y automatizar los procesos de copias de seguridad que se efectúe en el sistema. Soporte para todas las opciones necesarias en este tipo de software: comprimir las copias en formato .zip, encriptar con contraseña, actualización de archivos nuevos en la sobrescritura de copias.

MozBackup 1.5.1: Es una utilidad para crear copias de seguridad de Mozilla Thunderbird, Mozilla Firefox, Mozilla Suite. Su funcionamiento es muy simple. El programa detecta los programas "Mozilla" instalados y permite elegir crear una copia de seguridad "Backup a profile" o recuperar una realizada anteriormente (Restore a profile).

Uranium Backup 8.8.1: Programa que realiza copias de seguridad. Puede ser programado para realizar la copia un día en concreto a una hora en concreto, indicándole que carpetas o ficheros queremos incluir en la copia. El destino de la copia puede ser: disco externo, un CD o DVD, enviarla vía FTP. Además el programa se encarga de comprimir los datos, protegerlos con una contraseña y cifrarlos.

- **Navegadores de internet**

Un navegador es un software que permite acceder a Internet, interpretando el código de los archivos web y mostrando como resultado texto, imágenes, multimedia.

Ejemplo de navegadores de internet:

Internet Explorer 11: Es un Navegador desarrollado por Microsoft que presenta un aspecto renovado y características novedosas. Lo más llamativo es el cambio de la interfaz. La barra de direcciones y la caja de búsqueda se han fusionado, y el número de botones se ha reducido a tres. Ahora hay más espacio para navegar.

Mozilla Firefox 35.0: Navegador web libre y de código abierto, descendiente de Mozilla Application Suite y actualmente desarrollado por la Corporación Mozilla. Mozilla Firefox es uno de los navegador más utilizado de Internet, con una alta cuota del mercado.

Google Chrome 38.0.2125.111: Es un navegador web desarrollado por Google, es uno de los navegadores más usados en Internet y se caracteriza por su poco consumo de recursos. El nombre del navegador deriva del término usado para el marco de la interfaz gráfica de usuario ("chrome") (Hernández Ramírez, 2015).

4.3.2. Plan de seguridad establecido

Finalmente la realización del plan de seguridad para mitigar el riesgo informático encontrado en la empresa Fideval de un 27%, garantiza el éxito de la misma en cuestión de seguridad de sus activos y con él de su información.

Las siguientes medidas estarán incluidas en cada uno de los riesgos a los que se hará mención en este epígrafe además de las que se pondrán específicamente para cada uno de ellos:

1- Realizar una campaña de concientización entre todos los empleados de la empresa Fideval, desde los guardias de seguridad hasta los directores, que tenga por objetivo que la fuerza laboral:

a) Entienda qué es información confidencial, secreta, sensible o clasificada, y por qué dicha información guarda tal clasificación.

b) Conocer las consecuencias legales que pueden surgir si se comparte, se copia o se divulga dicha información, las cuales pueden ir desde una simple amonestación (acta administrativa), hasta el despido o inclusive penas económicas (daños y perjuicios) o corporales (prisión).

2- Todo empleado, sea directo o indirecto, debe tener en su contrato individual de trabajo dos cláusulas: la de confidencialidad de la información y la de protección de datos personales. Igualmente importante es tener estas cláusulas en los contratos con los proveedores de servicios y socios de negocios.

3- Elaborar políticas en la empresa que regulen el uso de recursos informáticos, redes sociales, información confidencial y privacidad. Estas políticas deben estar ligadas al Reglamento Interior de Trabajo o idealmente al contrato individual de trabajo de cada empleado. Ellos deben manifestar conocer dichas políticas y obligarse a su cumplimiento.

4- La empresa está obligada por ley a tener medidas de seguridad técnicas, físicas y administrativas para proteger sus datos contra robo, destrucción, alteración, uso o acceso no autorizado.

5- Si existe una vulneración de la información, se debe tener formulado un plan de reacción que incluya al menos:

a) La detección de la información vulnerada.

b) Establecer medidas correctivas y preventivas.

c) Dar aviso a los titulares cuyos datos personales pudieran haber sido comprometidos.

d) Aplicar sanciones laborales en caso de que exista responsabilidad o negligencia por parte de empleados.

6- Las contraseñas asignadas con varios fines, ya sea para archivos cuya información es de carácter vulnerable o en computadoras de la empresa que lo requieren, no deben ser transmitidas por medios no seguros como el teléfono ni ser compartidas con terceras personas que no la necesitan para desempeñar funciones en la empresa.

7- Establecer medidas de seguridad para la detección de intrusos en la red inalámbrica de la empresa. Las mismas pueden ser:

a) Cambiar la clave establecida para la misma en un tiempo promedio de 15 días utilizando una encriptación segura.
b) Observar constantemente las luces de actividad del router, pues si presenta un parpadeo continuado indica que hay dispositivos conectados transmitiendo un gran flujo de información.
c) Utilizar un software que ayude a detectar la actividad anormal existente en la red. El software recomendado es el AirSnare, el cual es una aplicación que corre en el entorno de Windows y brinda la oportunidad de escuchar una red determinada, mostrando los logs con los eventos que pasan a través del enrutador.

   AirSnare monitoria todas las direcciones MAC de las computadoras que se encuentran en la red y en un comienzo las detecta como desconocidas pero con la ayuda del personal que se encuentra a cargo

de este proceso se logra identificar cuáles de ellas pertenecen a la empresa y cuáles no para tomar medidas en base a ello (Geater, 2014).

4.3.2.1 Medidas específicas establecidas para cada activo con riesgo crítico.

- **Activo: Documentos institucionales**

Medidas:

1. Los documentos institucionales, al ser los instrumentos legales por los que se rige la empresa para su funcionamiento, deben estar concentrados en una computadora con medidas de seguridad preventivas y que contengan contraseñas robustas.

2. Esta contraseña solo debe estar en manos de trabajadores de la empresa que requieran trabajar con él directamente y que sea asignado por el director de la institución.

- **Activo: Finanzas**

Medidas:

1. Las computadoras que lleven el proceso de finanzas de la empresa deben estar bien respaldadas con cortafuegos.

2. Los archivos que tengan información vulnerable de la empresa en cuestiones de finanzas deben poseer contraseñas robustas que contenga una combinación de números, letras (mayúsculas y minúsculas) y caracteres especiales y que solo sea de conocimiento de la persona encargada y el director de la empresa.

- **Activo: Servicios bancarios**

Medidas:

1. Colocar un antivirus potente en cada máquina de la empresa.

2. No utilizar dispositivos USB ajenos a la empresa para evitar el contagio de virus.

3. Hacer salvas de la base de datos de los servicios bancarios periódicamente.

4. Establecer contraseñas robustas al paquete de datos trasmitidos que contenga una combinación de números, letras (mayúsculas y minúsculas) y caracteres especiales.

5. En caso de que se tenga la necesidad de enviar por la red información a otras empresas, fragmentarla en varios paquetes y en diferentes correos con contraseña.

6. La contraseña establecida solamente la puede conocer el máximo responsable de la información a enviar.

- **Activo: Respaldos**

Medidas:

1. El Backup tiene un propósito y es el estar preparados en caso de catástrofes de nuestros equipos, software, hurto, errores humanos o catástrofes naturales. En lo posible se debe guardar las copias de seguridad en diferentes lugares o poseer más de una copia, teniendo presente que las copias de igual forma pueden sufrir daños.

2. Establecer contraseñas robustas con la combinación de números, letras (mayúsculas y minúsculas) y caracteres especiales a los respaldos o backup de

información realizado y que esta solo sea del conocimiento del personal autorizado.

3. Instalar antivirus eficientes y activar permanentemente el cortafuego.

4. Establecer el orden de importancia de la información que se le realizará en el Backup.

5. Crear un plan de Backup lo cual es uno de los aspectos más importantes a tener en cuenta ya que es la hoja de ruta y establece los procedimientos, frecuencia y los horarios en los que se realizará el Backup, así como hacia dónde se enviarán las copias y quien es el responsable de esta tarea.

6. Se debe considerar las diferentes opciones de almacenamiento y escoger el medio o dispositivo de almacenamiento adecuado para nuestra empresa, desde un medio óptico DVD, cinta o disco duro que nos permita guardar las copias de seguridad que realicemos.

7. Se debe asegurar que la solución de Backup permita cifrar la información. De esta forma cuando el Backup salga de la compañía en caso de pérdida o robo de los medios la información se encontrará asegurada.

8. Validar las copias de seguridad lo cual ayuda a recordar los procedimientos y a verificar que el Backup esté disponible y se pueda realizar la recuperación con éxito (Herazo, 2012).

- **Activo: Datos e información no institucional**

Medidas:

1. La información no institucional debe ser manejada por el personal autorizado para este procedimiento con lo que se debe tener cuidados extremos.

2. Realizar salvas periódicas para la seguridad de la información y la integridad de los datos.

- **Activo: Cortafuegos**

Medidas:

1. Tener solamente instalado en las máquinas de la empresa un solo cortafuegos, pues no se necesita más de uno ejecutándose en una misma computadora.

2. Al elegir el cortafuegos a utilizar en la empresa, leer detenidamente su manual, puesto que cada producto tiene su propia forma de funcionar y sistema de configuración, lo que definirá toda la seguridad del mismo. Esta función debe ser realizada por alguien que comprenda perfectamente los objetivos propuestos y los medios para conseguirlos.

3. Dar mantenimiento al cortafuego periódicamente para vigilar el correcto funcionamiento del sistema.

- **Activo: Servidores**

Medidas:

1. El servidor de aplicaciones no debe ser accesible físicamente por cualquier persona.

2. Es conveniente que exista un espacio físico donde se ubique el servidor, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su funcionamiento, como la temperatura ambiental indicada.
3. En este espacio, además de ubicar el servidor, se pueden ubicar los elementos más sensibles de la red corporativa como el HUB/Switch y el servidor proxy.
4. Instalar un sistema de detección de intrusos para monitorear los accesos o tentativas a la red corporativa.

5. Capacitar el personal que trabaja directamente con el servidor en el trabajo de estos sistemas y herramientas.

- **Activo: Computadoras- Portátiles**

Medidas:

1. Realizar copias de seguridad de los dispositivos: Algunos empleados se llevarán sus equipos fuera de la oficina y con ello aumenta el riesgo de que el equipo se estropee, se pierda. Hay que asegurarse de que se tienen copias bajo control de la información contenida en los mismos.

2. Proteger los documentos importantes que están el equipo: Es necesario comprobar que los documentos importantes están protegidos y, aunque el dispositivo se pierda, no se corre el riesgo de perder datos críticos especialmente si son datos regulados y vulnerables.

3. Establecer cámaras de circuito cerrado dentro de la empresa Fideval donde se observe cada establecimiento por un personal contratado las 24 horas en caso de robo.

- **Activo: Programas de administración (contabilidad, manejo de personal)**

Medidas:

1. Los programas de administración deben poseer contraseñas robustas con la combinación de números, letras (mayúsculas y minúsculas) y caracteres especiales.

2. Estos programas de administración solo debe estar en manos del personal que trabaja con él y que de esta forma responda por su buen funcionamiento y fidelidad de información.

- **Activo: Junta directiva.**

Medidas:

1. Las medidas que sean tomadas en la junta directiva deben ser solamente de conocimiento de los implicados en la reunión, pues en caso de que tenga que saberlo el personal de la empresa se les informará en el momento indicado.

2. Las actas digitales que contienen la información acordada en la junta debe poseer contraseña y solamente debe estar en la computadora de las personas seleccionadas.

- **Activo: Dirección/coordinación**

Medidas:

1. La dirección de la empresa debe tener un equipo de informáticos a cargo del manejo y mantenimiento de todas las máquinas de la institución. Estos trabajadores deben mantener informado a la dirección de todo lo novedoso que gira en función de estos aspectos.

2. Las computadoras de los directivos deben poseer una clave de administración que solo puede ser del conocimiento de ellos para su seguridad.

CAPÍTULO 5

CONLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

En la presente investigación se realizó un análisis de riesgos informáticos para disminuir el impacto sobre los activos de la empresa Fideval, mediante el uso del estándar ISO 27001.

Una vez concluidas las principales tareas que forman este proyecto, es el momento en el que se puede hacer balance y crítica de los resultados obtenidos. Así pues, repasando los objetivos inicialmente marcados se tienen las siguientes conclusiones:

1. Se identificaron y catalogaron los activos de la empresa los cuales representaban una magnitud de daño en la escala de uno a cuatro, según la categoría a la que pertenecían.

2. Se trabajaron en el desarrollo de la investigación solo los activos que son considerados como riesgos críticos por su nivel de importancia y de consecuencias negativas que pudieran traer a la empresa. Los mismos se distribuyeron, según las características de los activos en las siguientes categorías: datos, sistemas y personal.

3. Se identificaron las amenazas en la empresa Fideval y se distribuyeron en las diferentes categorías: actos originados por la criminalidad común y motivación política, sucesos de origen físico y sucesos derivados de la impericia, negligencias de usuarios y decisiones institucionales. Las

mismas se encuentran catalogadas con probabilidad de ocurrencia insignificante, baja, mediana y alta.

4. Se identificaron las vulnerabilidades del sistema, atendiendo a la ponderación de la amenaza.

5. Se utilizaron las técnicas de valoración para el cálculo del impacto y riesgo según la norma ISO 27001, la cual se consideró la más adecuada para realizar este proceso, ya que ayuda a descubrir los activos con riesgo de la empresa y planificar medidas oportunas para que se mitiguen los mismos.

6. Se calculó el impacto y el riesgo para los activos identificados en la empresa Fideval, ya que es necesario mantener la seguridad de la empresa en sus aspectos de confidencialidad, integridad y disponibilidad para asegurar el correcto funcionamiento de la organización.
7. Se elaboró un plan de seguridad en la empresa Fideval, para cada uno de los activos encontrados con riesgos críticos.

5.2 RECOMENDACIONES

1. Tomar en cuenta como estudio final los activos que son considerados con baja posibilidad de riesgos informáticos, ya que como prioridad se trabajarán los que son considerados como riesgo crítico.
2. Realizar un estudio mensualmente para determinar futuros riesgos por cada área de la empresa.

3. En el proceso de detección de amenazas y vulnerabilidades de los activos realizar una correcta ponderación de estos.
4. Utilizar los valores obtenidos del cálculo del impacto y el riesgo con el fin de certificar la empresa Fideval.
5. Implementar el plan de seguridad diseñado.

BIBLIOGRAFÍA

Acuña, N. (2014). Trabajo De Mantenimiento. 6.

Borek, A. (2013). *Gestión de riesgos de la información.* New York: Elsevier.

Calder, A. (2005). *Seguridad en la información.* Londres: Kogan Page.

Cano, F. (05 de Junio de 2012). *SEINHE. Consultores, auditores e ingenieros de seguridad informática.* Recuperado el 23 de Enero de 2015, de http://www.seinhe.com/blog/64-gestion-de-activos-de-ti

Corlleti, A. (20 de Frebrero de 2006). *ISO 27001: Los controles*. Obtenido de ISO 27000 en español: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf

Dávalos Ávila, J. C., & Bonilla Arroyo, P. (2007). *Prototipo de impresora para modelos 3D en cera.* SANGOLQUÍ.

Fideval. (01 de 01 de 2014). *¿Quiénes somos?* Obtenido de Fideval: http://www.fideval.com/index.php?page=2&&language=es

Galdamez, P. (07 de Marzo de 2006). *Seguridad Informática.* Obtenido de Instituto tecnológico de informática: Instituto tecnológico de informática

Geater, J. (2014). ¿Qué es AirSnare. exe y como solucionarlo? *Solvusoft*, 7.

Gutierrez Amaya, C. (2012). ¿Qué es y por qué hacer un Análisis de Riesgos? *Welifesecurity*, 3.

Herazo, J. C. (2012). Que es Backup y que se debe tener en cuenta . 5.

Hernández Ramírez, C. (2015). *PROGRAMAS DE SEGURIDAD INFORMÁTICA*. Obtenido de PROGRAMAS DE SEGURIDAD INFORMÁTICA: http://www.seguridadpc.net/programas/

ISO / IEC. (2009). *Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Ginebra: ISO.

ISO 27000 en español. (09 de Noviembre de 2014). *SGSI*. Obtenido de ISO 27000 en español: http://www.iso27000.es/sgsi.html

ISO 27001 Standards. (08 de Marzo de 2013). *Lista de documentación obligatoria requerida por ISO/IEC 27001* . Obtenido de ISO 27001 Standards: http://www.iso27001standard.com/es/que-es-iso-27001/

Kosutic, D. (2015). ¿Qué es norma ISO 27001? *Academy*, 5.

Kouns, J. (2010). *Information technology risk management.* Hovoken, NJ: Jhon Wiley & Sons.

Monachesi, E., & Frenz, A. M. (2011). *Efecto de la Foresta en las Transmisiones electromagnéticas dentro de una WLAN. Conceptos generales de antenas.* Universidad Tecnológica Nacional .

Organización Internacional de Estandarización. (2005). *ISO/IEC 27001.* New York: ISO.

Organización Internacional de Estandarización. (2005). *ISO/IEC 27002.* New York: ISO.

Peltier, T. (2005). *Análisis de riesgos en seguridad informática.* Boca Ratòn: CRC Press.

Pérez Valdéz, D. (2007). ¿Qué son las bases de datos? 10.

Vicuña, M. (2011). *Efectos de los Virus en las Computadoras.* Universidad Simón Rodríguez.

Wheeler, E. (2011). *Gestión de riesgo: Construyendo un programa de gestión de riesgos.* Wollongong: Syngress - Elsevier.