ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL FONDO DE CESANTÍA Y JUBILACIÓN DEL MDMQ.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

ABALCO MAILA DAVID ELÍAS

davidelias_am@hotmail.com

RUILOVA SANDOVAL ROMEL RUPERTO

romel.ruilova@gmail.com

DIRECTOR: MSC. ING. GABRIELA LORENA SUNTAXI OÑA

gabriela.suntaxi@gmail.com

Quito, Abril 2015

DECLARACIÓN

Nosotros, David Elías Abalco Maila y Romel Ruperto Ruilova Sandoval, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

David Elías Abalco Maila

Romel Ruperto Ruilova Sandoval

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por David Elías Abalco Maila y Romel Ruperto Ruilova Sandoval, bajo mi supervisión.

Msc. Ing. Gabriela Suntaxi

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Primeramente quiero agradecer a Dios por darme la salud, la fuerza y la sabiduría necesaria que me han permitido alcanzar este nuevo logro.

Agradezco a mi madre por su apoyo incondicional a lo largo de toda mi vida, a mi Familia que siempre me ha sabido guiar por un buen camino, al Ing. Willam Castillo Administrador del Fondo de Cesantía y Jubilación quien nos ha permitido llevar a cabo la realización de este proyecto, a la Ing. Gabriela Suntaxi quien nos brindado todo su apoyo y nos ha sabido guiar adecuadamente en el transcurso del mismo y finalmente quiero agradecer a mis compañeros y amigos quienes también han sido parte fundamental en mi formación como persona y como profesional.

David Elías Abalco Maila

AGRADECIMIENTOS

En primer lugar, doy gracias a Dios por brindarme la fuerza, paciencia, constancia y conocimientos necesarios para superar los obstáculos que se presentaron a lo largo de este complicado camino hacia la obtención de mi carrera profesional.

A mi madre, mi padre y mis hermanos, quienes me han brindado su apoyo incondicional, su cariño y su amor en los buenos y malos momentos para seguir adelante y no desfallecer en el cumplimiento de mis objetivos y metas.

A mis abuelitas, mis tías, mis tíos, mis padrinos y el resto de mi familia, por todos sus consejos, buenos deseos y por estar pendientes de mí en todo momento.

A la Ing. Gabriela Suntaxi, por su apoyo, colaboración, paciencia y tiempo brindado para el desarrollo de este proyecto, demostrando su calidad humana y profesional.

Al Ing. Willam Castillo y al Ing. Juán Suarez, por brindarnos la apertura y respaldo necesario en la realización de este proyecto.

A mis amigos y amigas, por estar siempre presentes en los buenos y malos momentos brindándome su apoyo y buenas energías para superar las dificultades y pruebas que nos pone la vida día a día.

Y finalmente, quiero agradecer a una chica maravillosa quien desde que la conocí se ha convertido en parte importante de mi vida. Con su sola presencia me ha brindado momentos de felicidad y tranquilidad al saber que cuento con ella.

Romel Ruperto Ruilova Sandoval

DEDICATORIA

Dedico este proyecto a mi madre por todo su esfuerzo realizado a lo largo de mi carrera.

David Elías Abalco Maila

DEDICATORIA

El presente trabajo va dedicado a las siguientes personas importantes en mi vida:

A mi madre y mi padre por brindarme todo su amor, paciencia y preocupación por mi bienestar en todos los sentidos en que lo pueden hacer los padres que desean ver que sus hijos se superen en la vida. Por constituirse en un ejemplo a seguir y demostrarme los valores, principios y cualidades que una persona de bien debe poseer para sobresalir ante la sociedad.

A mis hermanos, por ser el motivo para seguir superándome y convertirme en su ejemplo y razón de orgullo. Espero que en el futuro ellos logren superar todo lo que he alcanzado en mi actual carrera profesional.

A toda mi familia en general, por apoyarme de una u otra manera en los buenos y malos momentos de mi vida.

Romel Ruperto Ruilova Sandoval

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Actualmente, las organizaciones han sobrestimado la temática sobre seguridad de la información por múltiples razones, ya sea por desconocimiento, por considerarlo un tema tedioso o simplemente por no considerar necesaria su implementación para controlar las actividades cotidianas que realizan sus empleados.

Debido a la falta de interés en dicho tema, se han suscitado grandes pérdidas de información importante que han afectado enormemente tanto a organizaciones públicas como privadas, razón por la cual se hace imprescindible dar a conocer la importancia de implementar normas como la NTE INEN-ISO/IEC 27001:2011 para garantizar la seguridad necesaria sobre los activos que posee la organización.

Complementario a la norma mencionada, existen múltiples metodologías para la evaluación de riesgos como son: OCTAVE, RISK IT, MAGERIT, entre otras. Con las cuales se puede determinar el grado de impacto que tendría el no implementar los controles y medidas necesarias para garantizar la protección de los activos críticos.

Por lo que, el presente proyecto pretende brindar una visión general sobre la identificación, evaluación y tratamiento de los riesgos que comprometen la integridad y seguridad de los activos de la organización. Para lo cual, se establece la implementación de políticas y controles que ayudarán a que el personal de la organización se familiarice con la temática y la importancia de la seguridad de la información.

Finalmente, se tendrá como resultado el Plan de Seguridad de la Información, el cual será susceptible a cambios, revisiones y mejoras, según lo consideren las autoridades correspondientes a quienes va dirigido este entregable.

RESUMEN

El presente proyecto de titulación consta de cuatro capítulos que abarcan los siguientes puntos: Planteamiento del problema, Elaboración del plan de seguridad, Evaluación de la aplicabilidad del plan de seguridad y finalmente conclusiones y recomendaciones para el Fondo de Cesantía y Jubilación.

El Capítulo 1 contiene una descripción completa de la caracterización de la empresa así como también se describe la problemática del estado actual de la misma en cuanto a seguridad de la información. Este capítulo también presenta una breve descripción de la Familia ISO 27000 y se detallan las ISO 27001, 27003 y 27005 que serán utilizadas para la elaboración de este proyecto.

El Capítulo 2 identifica los problemas encontrados de acuerdo a cada dominio de la norma ISO27001. Luego, para la evaluación de riesgos es necesario describir brevemente varias metodologías (OCTAVE, RISK IT, NIST 800-30 y MAGERIT), comparar cada una de ellas, seleccionar la metodología más adecuada y finalmente aplicar cada una de las fases que proponga la metodología seleccionada. En este caso la metodología utilizada para la Evaluación de Riesgos ha sido MAGERIT la cual consta de las siguientes fases: Identificación del activo crítico, Identificación de amenazas asociadas a los activos, Identificación y valoración de vulnerabilidades, Identificación y valoración de impactos, Estimación del riesgo y Manejo y tratamiento del riesgo. Una vez que se hayan cumplido con todas estas fases se procede con la elaboración de las políticas de seguridad de la información de acuerdo a los controles establecidos en la fase final de MAGERIT. Para finalizar con este capítulo se establecerá un escenario el cual permitirá validar el Plan de Seguridad de la Información mediante la implementación de una política dentro del Fondo de Cesantía y Jubilación.

El Capítulo 3 presenta una comparación del porcentaje de cumplimiento actual y el que se espera luego de la implementación del Plan de Seguridad de la Información,

tomando en cuenta como referencia el porcentaje de cumplimiento por cada dominio de la norma ISO 27001 dentro de la organización. Seguidamente se realizará un breve análisis de las restricciones de tiempo, financieras, técnicas, de personal y políticas que pueden dificultar la implementación del Plan de Seguridad de la Información, pero también se proporcionarán soluciones a dichas restricciones para que este Plan pueda ser implementado. Este capítulo también pretende dar a conocer los recursos que serán necesarios para llevar a cabo la implementación del Plan de Seguridad de la Información mediante un análisis la factibilidad técnica, operacional y económica. Finalmente se cuenta con un conjunto de actividades ordenadas sistemáticamente que hacen posible la implementación del Plan de Seguridad de la Información.

El Capítulo 4 contiene las conclusiones y recomendaciones obtenidas en el transcurso de este proyecto.

1 PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DE LA EMPRESA

A continuación haremos una breve descripción de los lineamientos principales en los cuales se sustenta el Fondo de Cesantía y Jubilación.

1.1.1 RESEÑA HISTÓRICA

El Municipio del Distrito Metropolitano de Quito, bajo la administración del Dr. Jamil Mahuad Witt, llevó adelante la creación del Fondo de Jubilación Patronal Especial (FJPE), el mismo que se constituye para garantizar económicamente la condición de vida de quienes se acojan a este beneficio.

El Fondo de Jubilación Patronal Especial de los funcionarios, empleados y trabajadores del MDMQ; y, sus empresas EPMMOP y EMASEO, se crea mediante Ordenanza N° 3109 del Consejo Metropolitano de Quito, el 15 de abril de 1994.

El Consejo Metropolitano incorpora en el Código Municipal a la ordenanza mencionada, mediante la Ordenanza N° 001 del 3 de septiembre de 1997 en el Registro Oficial N° 226 del 31 de diciembre de 1997, llevando consigo algunas modificaciones.

En el Registro Oficial N° 325 del 1 de agosto del 2006 se expide la ordenanza reformatoria a la Sección XII del Capítulo II del Libro Primero del Código Municipal, relacionado con los integrantes del Directorio y el tiempo para acogerse a la jubilación por vejez.

La Superintendencia de Bancos y Seguros, mediante resolución N° SBS-2007-196 del 7 de marzo del 2007, aprueba el Estatuto.

En su creación, el Fondo fue financiado por una contribución inicial de $15.000’000.000 (QUINCE MIL MILLONES DE SUCRES 00/100) netos, entregados por el Gobierno Nacional, equivalente a la reserva matemática por los años de

trabajo anteriores al 31 de diciembre de 1992, de todos los servidores del Municipio Metropolitano de Quito, según los cálculos matemáticos actuariales.

La Superintendencia de Bancos y Seguros, mediante Oficio INSS-2008-309, solicita a los Fondos Previsionales Cerrados, el registro de los aportes de los partícipes en cuentas individuales, a fin de garantizar un apropiado y transparente manejo de las cuentas de ahorro para lo cual se pasaría de un Sistema Solidario a un Sistema de Cuentas Individuales, así los partícipes serían acreedores de los recursos que tienen acumulado en sus cuentas (aportes + intereses).

Con la creación de la Ley Orgánica de Empresas Públicas se prohíbe el aporte a Fondos de Cesantía o Jubilación con recursos públicos, con lo cual se vio mermado el ingreso de recursos para el financiamiento del Fondo, ya que se dejó de percibir los aportes patronales de las empresas.

El Fondo es de carácter privado y a partir del año 2004 se incorpora las iniciales FCPC que significa Fondo Complementario Previsional Cerrado, según la resolución No. SBS-2004-0740 de la Superintendencia de Bancos y Seguros.

El grupo asegurado está conformado por:

- Los funcionarios, empleados y trabajadores del Municipio del Distrito Metropolitano de Quito y de sus empresas: EPMMOP y EMASEO.
- Los funcionarios, empleados y trabajadores que mediante nombramiento expedido por el Señor Alcalde Metropolitano de Quito, cumplan funciones o trabajos remunerados en el Municipio Metropolitano desde el primer día de iniciar sus labores.

1.1.2 MISIÓN, VISIÓN, OBJETIVOS, ESTRATEGIAS, PRINCIPIOS Y VALORES

Misión

Administrar con transparencia, eficiencia y eficacia los recursos económicos, para la concesión oportuna de prestaciones y servicios a nuestros partícipes y pensionistas por vejez, invalidez y muerte.

Visión

Capitalizar los recursos económicos con que cuenta el Fondo de Jubilación para mantener una sostenibilidad a futuro en las prestaciones de vejez, invalidez y muerte.

Objetivos

- Reducir los procesos, utilizando tecnología de punta para entregar un servicio oportuno a los beneficiarios.
- Generar alternativas de ingreso e inversión para incrementar el capital del Fondo y otorgar pensiones dignas a sus jubilados.

Estrategias

- Programar la jubilación de los partícipes, para evitar una descapitalización del Fondo.
- Colocar a través de prestaciones, el tope máximo permitido para una institución de este tipo, y obtener alta rentabilidad con reducido riesgo.
- Invertir los excedentes en el mercado financiero, procurando obtener rendimientos altos y seguros, en plazos adecuados.
- Crear una provisión anual que contrarreste el latente riesgo de una reducción o eliminación de los aportes patronales por parte del MDMQ.
- Estructurar al Fondo para que cuente con todos los niveles administrativos, financieros, planificación, control, etc., de manera que se alcance el fortalecimiento institucional.

Principios

Los principios fueron sometidos a consideración y selección por parte de los empleados.

- **Inclusión:** Oportunidad que brinda la entidad para una participación activa dentro de la misma.
- **Equidad Social:** Balance intercultural y de género en la toma de decisiones.

- **Obligatoriedad:** Compromiso de obrar bajo la necesidad de cumplir.
- **Suficiencia:** Competencia, habilidad y capacidad para realizar las actividades de cada área.
- **Integración:** Reunión de personas de diferentes grupos sociales para perseguir un mismo objetivo o precepto.

Valores

La selección de valores se realizó con ayuda de una encuesta aplicada al grupo que participó en los talleres de Planificación Estratégica y Balance Scorecard, escogieron de quince valores, los más utilizados a nivel de empresas e instituciones de carácter social, los considerados estaban mayormente familiarizados con la misión y visión del Fondo y son los siguientes:

- **Responsabilidad:** Dedicación y esmero en el desenvolvimiento de las tareas encomendadas por más simples que resulten ser.
- **Calidad:** Superioridad o excelencia en la tarea encargada.
- **Respeto:** Justicia y valor por los demás.
- Confidencialidad: Lo que se hace o dice de manera reservada, esperando reciprocidad.
- **Honradez:** Renuncia voluntaria y sin remordimientos hacia cualquier cosa que no sea de nuestra propiedad.
- **Solidaridad:** Sentimiento de apoyo hacia cualquier desavenencia que le pueda ocurrir a nuestros semejantes.

1.1.3 ANÁLISIS FODA

El análisis FODA, es una metodología de estudio sobre la situación real de una entidad cuyo diagnóstico será la base para planificar una estrategia de futuro mediante la toma de decisiones que estarán acordes con los objetivos que persigue la organización.

Este análisis determina como factores internos: fortalezas y debilidades; y, como factores externos: oportunidades y amenazas, que merecen ser examinados para

establecer las acciones pertinentes que servirán como punto de partida para alcanzar el éxito de la entidad.

El Fondo de Jubilación Y Cesantía ha determinado el FODA institucional con la participación de todo su personal y la contratación de un profesional en el tema, a continuación se presenta los resultados:

Figura 1.1 Análisis FODA
Fuente: Fondo de Cesantía y Jubilación

Fortalezas

- Capacidad económica financiera para desarrollar nuevos productos de inversión.

- Flujo permanente de ingresos provenientes de la aportación de los partícipes y recuperación de cartera.
- El recurso humano cuenta con un perfil idóneo para ejecutar las actividades en el área que se desenvuelve.
- Cartera sana por apoyo de las empresas municipales.
- Capacitación al personal de todas las áreas.

Debilidades

- Carencia de manuales y políticas en cada área de la entidad.
- Oficinas inadecuadas para clientes internos y externos.
- Falta de normativa para actualizar la base de cotización.

Oportunidades

- Adecuación de la normativa interna del Fondo.
- Celebración de nuevos contratos de portabilidad.
- Ingreso voluntario de nuevos partícipes.
- Adquisición de un nuevo sistema informático.
- Alianzas estratégicas con entidades de variado tipo.

Amenazas

- Reducción de aportes patronales.
- Políticas gubernamentales.

1.1.4 ORGANIGRAMA ESTRUCTURAL

La Figura 1.2 que podemos ver a continuación nos muestra una visión simplificada de los niveles jerárquicos y la relación que existe entre ellos, su propósito es brindar información sencilla de utilizar y fácil de comprender en lo que respecta al Fondo de Cesantía y Jubilación.

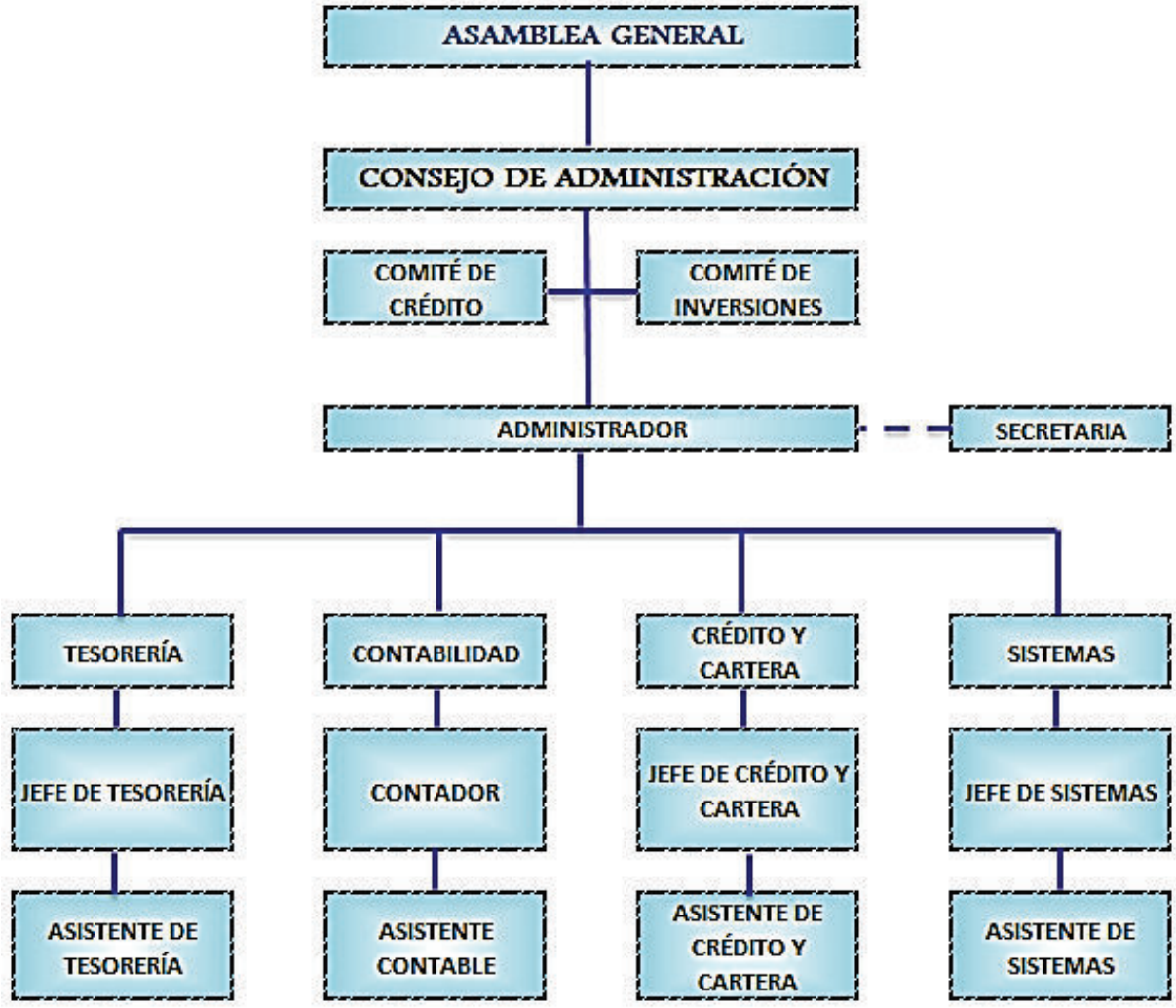

Figura 1.2 Organigrama Estructural
Fuente: Fondo de Cesantía y Jubilación

1.1.5 ÁREA DE TI

El área de sistemas es un área de apoyo que facilita a sus procesos más importantes, ser gestionados de manera adecuada.

1.1.5.1 Misión y Visión

Misión

Tener al día y de una manera ordenada, sistemática y lógica el manteamiento de la infraestructura, del software y de los contratos con los proveedores.

Visión

Mantener al fondo en las políticas y estándares de tecnología e infraestructura activos.

1.1.5.2 Organigrama del departamento de sistemas

La Figura 1.3 nos muestra como se encuentra estructurada el área de sistemas, a continuación podemos observar que este departamento solo cuenta con dos niveles de jerarquía que se relacionan directamente, muy sencillos y fáciles de comprender.

Figura 1.3 Organigrama del Departamento de Sistemas
Fuente: Fondo de Cesantía y Jubilación

1.1.5.3 Descripción de responsabilidades del personal de sistemas

La tabla 1.1 describe el cargo, puesto, perfil y experiencia, funciones y perfil por competencias de la persona que se encuentra ocupando el cargo de Analista de Sistemas.

DESCRIPCIÓN DEL CARGO			
PUESTO:	Jefe de Sistemas	**LUGAR:**	MDMQ
REPORTA:	Administrador	**AREA:**	Sistemas
DESCRIPCIÓN DEL PUESTO			
Apoyar oportunamente en la prestación de servicios de calidad que brinda el Fondo, en cuanto a la administración de la información financiera y operativa de la institución, mediante la implementación, evaluación, mejoramiento y			

actualización de los sistemas informáticos y los procesos que estos abarcan.

PERFIL Y EXPERIENCIA ACADÉMICA

Título de Ingeniero de Sistemas o Tecnólogo en Sistemas otorgado por una institución de nivel superior.
3 años en cargos similares.

FUNCIONES DEL PUESTO

a) Mejorar la calidad de la información existente mediante revisiones a reportes, datos y aplicaciones.
b) Cumplir con las disposiciones de los Organismos de Control y realizar el seguimiento a las observaciones y recomendaciones emitidas por Auditoría Externa, Superintendencia y a través de los informes de Auditoría Interna.
c) Elaborar y actualizar los manuales de sistemas y las políticas de seguridad.
d) Evaluar los servicios de comunicaciones en todas las oficinas del Fondo.
e) Evaluar y hacer cumplir los acuerdos de servicios tercerizados y realizar seguimientos contractuales.
f) Analizar y evaluar la adquisición e implementación de Proyectos de Tecnología enfocados a la mejora de servicio en el Core Financiero y los servicios de TI.
g) Cumplimiento del Plan Operativo, y cumplimiento de las Resoluciones de los Organismos de Control, Internos y Externos.
h) Garantizar y verificar el correcto funcionamiento del sistema informático financiero y coordinar acciones con el proveedor para corregir eventuales errores que el sistema pueda arrojar.
i) Realizar el análisis de requerimientos de desarrollo de aplicaciones referente al sistema informático financiero provenientes de usuarios autorizados, priorizar los mismos en base a importancia crítica del requerimiento y hacer recomendaciones para ajustar cronogramas y recursos necesarios.
j) Coordinar el desarrollo y ejecución de las actividades de mantenimiento preventivo y correctivo de equipos de computación y UPS.
k) Coordinar el soporte en cuestiones de hardware, software y sistema financiero

con los respectivos usuarios.

l) Diseñar y actualizar diferentes políticas para la administración de los centros de cómputo.

m) Dar soporte técnico sobre los módulos del sistema financiero contable.

n) Proponer la implantación de nuevas tecnologías existentes, métodos, procedimientos, técnicas administrativas que permitan optimizar la gestión empresarial.

o) Diseñar, proponer y ejecutar el Plan Estratégico de Sistemas de Información y Comunicaciones.

p) Llevar un control de los equipos de computación en lo referente al hardware y software.

q) Administrar la infraestructura de comunicación, servidores y redes de los fondos.

r) Realizar cambios en los diferentes sistemas que usen los diferentes fondos.

s) Mitigar el impacto en el funcionamiento de los diferentes sistemas, cuando suceda un imprevisto.

t) Realizar periódicamente respaldos de base de datos, así como de otros dispositivos de memoria.

u) Analizar, recomendar, administrar y monitorear proyectos completos, referentes al área de sistemas, así como la parte de informática de otros proyectos no referentes.

v) Administrar actualizaciones de diferentes sistemas informáticos.

w) Generar documentación necesaria para entes de control (SBS).

x) Administración de documentación de diferentes aspectos, que se detallan:

   a. Manuales técnicos.

   b. Manuales de usuario.

   c. Manuales estratégicos.

y) Administración de la herramienta en la cual se desarrolla el plan estratégico.

z) Revisión y realización de informes periódicos referentes al área, en aspectos económicos, técnicos y capacitación.

PERFIL POR COMPETENCIAS

CONOCIMIENTOS INDISPENSABLES:

- Conocimiento actualizado en herramientas de Tecnología de Información y Comunicaciones.
- Sistemas Operativos (WINDOWS, LINUX, u otros).
- Infraestructura de Redes LAN y WAN
- Administración y estructura de BDD, SYBASE u otras.
- Conocimiento de programación a nivel medio.
- Técnicas de Help-Desk.
- Conocimientos en el Sistema Informático Financiero Contable que este en vigencia a nivel de usuario y técnico.
- Conocimiento de lenguaje de programación Java.
- Base de datos Oracle, SQL Server 2005
- Administración y gerencia de proyectos de desarrollo de sistemas.
- Conocimientos de Seguridad Informática.

DESTREZAS GENERALES:

- Juicio y toma de decisiones.
- Organización de sistemas.
- Programación.
- Identificación y reconocimiento de problemas.
- Conocimiento básico de inglés técnico.
- Conocimientos de procesos.
- Conocimiento de administración de riesgos.

OTRAS COMPETENCIAS:

- Originalidad.
- Razonamiento inductivo y deductivo.
- Agilidad.
- Capacidad de análisis.
- Negoción.

INDICADORES DE GESTIÓN

➢ Cumplimiento Plan Operativo = Actividades cumplidas / Actividades programadas

Tabla 1.1 Descripción de Responsabilidades del Personal de Sistemas
Fuente: Fondo de Cesantía y Jubilación

La tabla 1.2 describe el cargo, puesto, perfil y experiencia, funciones y perfil por competencias de la persona que se encuentra ocupando el cargo de Auxiliar de Sistemas.

DESCRIPCIÓN DEL CARGO			
PUESTO:	Asistente de Sistemas	**LUGAR:**	Matriz
REPORTA:	Jefe de Sistemas	**AREA:**	Sistemas
DESCRIPCIÓN DEL PUESTO			
Asistir en Informática y Tecnología en el desarrollo y ejecución de diversos proyectos y actividades relacionadas con la gestión tecnológica del área.			
PERFIL Y EXPERIENCIA ACADÉMICA			
Cursando los últimos años en Ingeniería de Sistemas. De 6 a 12 meses en posiciones similares.			
FUNCIONES DEL PUESTO			
a) Implantar y facilitarla utilización de paquetes informáticos de propósito general y aplicaciones específicas. b) Proponer y coordinar cambios para mejorar la explotación del sistema y las aplicaciones. c) Nuevos desarrollos: análisis, programación y documentación. d) Mantenimiento de aplicaciones: corrección de errores, adaptación de los programas a nuevas necesidades (nuevas normativas, cambios organizativos, etc.) e) Soporte sobre los desarrollos o actualizaciones a los sistemas informáticos. f) Apoyo técnico a la dirección y servicios-unidades. g) Responsable de la elaboración y mantenimiento de los sistemas que se manejan con la aplicación.			

h) Responsable de los paquetes instalados con la aplicación.
i) Interpretar las necesidades de los usuarios y confeccionar las soluciones pertinentes.
j) Encargado de investigar y probar nuevos productos para la aplicación.
k) Responsable de la integridad de la información que se genera y manipula con la aplicación.
l) Se encarga de los controles de los sistemas y programas informáticos.
m) Realizar copias de seguridad de datos.
n) Realizar copias de seguridad de los programas y fuentes del sistema financiero.
o) Aplicar actualizaciones del sistema operativo y generar los cambios de configuración en coordinación con el proveedor del hardware.
p) Monitorear el rendimiento del sistema financiero.
q) Controlar y respaldar las versiones que se implementen.
r) Responder a las consultas de carácter técnico.
s) Documentar la configuración del sistema.
t) Afinar el rendimiento de los sistemas.
u) Todos aquellos requerimientos que se presenten en el departamento.
v) Enviar un informe de las actividades y las asistencias técnicas realizadas.

PERFIL POR COMPETENCIAS

CONOCIMIENTOS INDISPENSABLES:

- Conocimiento Hardware, Software a nivel avanzado.
- Conocimiento de programación a nivel avanzado.
- Conocimiento de Redes a nivel avanzado.
- Administración de Sistemas Operativos (WINDOWS, LINUX u otros).
- Conocimiento de la Administración de Base.
- Conocimiento de Programación.

DESTREZAS GENERALES:

- Escucha Activa.
- Identificación de problemas.

➢ Operación y control. ➢ Detección de averías. ➢ Mantenimiento de equipos. ➢ Destrezas científicas. ➢ Programación. ➢ Administración del tiempo. ➢ Orientación a resultados. **OTRAS COMPETENCIAS:** ➢ Razonamiento inductivo y deductivo. ➢ Destreza manual. ➢ Tolerancia. ➢ Ordenar información. ➢ Iniciativa. ➢ Capacidad analítico-sintética. ➢ Conocimiento del idioma quichua y español.
INDICADORES DE GESTIÓN
➢ Cumplimiento Plan Operativo = Actividades cumplidas / Actividades programadas

Tabla 1.2 Descripción de Responsabilidades del Personal de Sistemas
Fuente: Fondo de Cesantía y Jubilación

1.1.5.4 Diagrama de Red

La Figura 1.4 nos muestra cómo se encuentran conectados los equipos, el nombre del responsable de cada uno de ellos, su respectiva dirección IP y el área a la cual pertenecen.

Como podemos apreciar el Fondo de Cesantía y Jubilación cuenta con tres servidores: Un servidor de correo y dos servidores de base de datos, en el servidor de correo se encuentran almacenados los archivos de correo internos de la organización, además este utiliza la herramienta webmin para controlar toda la red de internet. El servidor de base de datos Windows Server 2000 (IBM) contiene y almacena la información de: hipoteca, crédito y aportes de cesantía, la contabilidad

de cesantía y jubilación y el kardex (registro de manera organizada de todos los activos fijos de la organización). El servidor de base de datos Windows Server 2000 (Compaq) contiene y almacena la información de: crédito y aportes de jubilación y cheques de jubilación.

Adicionalmente tenemos otro servidor que no se encuentra en la Figura debido a que este solo se usa para realizar pruebas de un nuevo sistema que se encuentra en desarrollo en el Fondo de Cesantía y Jubilación.

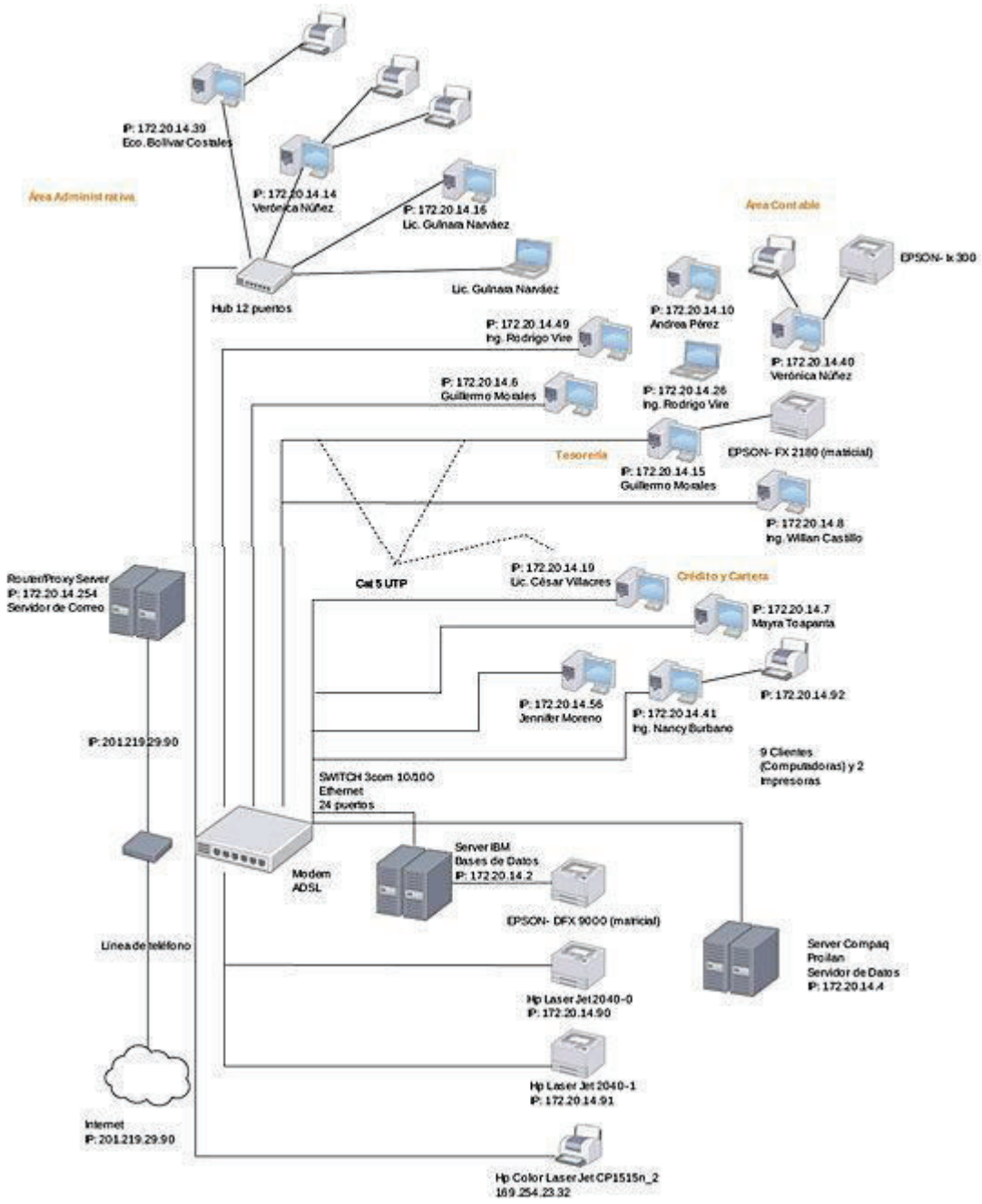

Figura 1.4 Diagrama de Red
Fuente: Fondo de Cesantía y Jubilación

1.1.6 DIAGRAMA FÍSICO DE LA ORGANIZACIÓN

En la Figura 1.5 podemos observar la ubicación de cada departamento y la distribución de todos sus equipos tecnológicos.

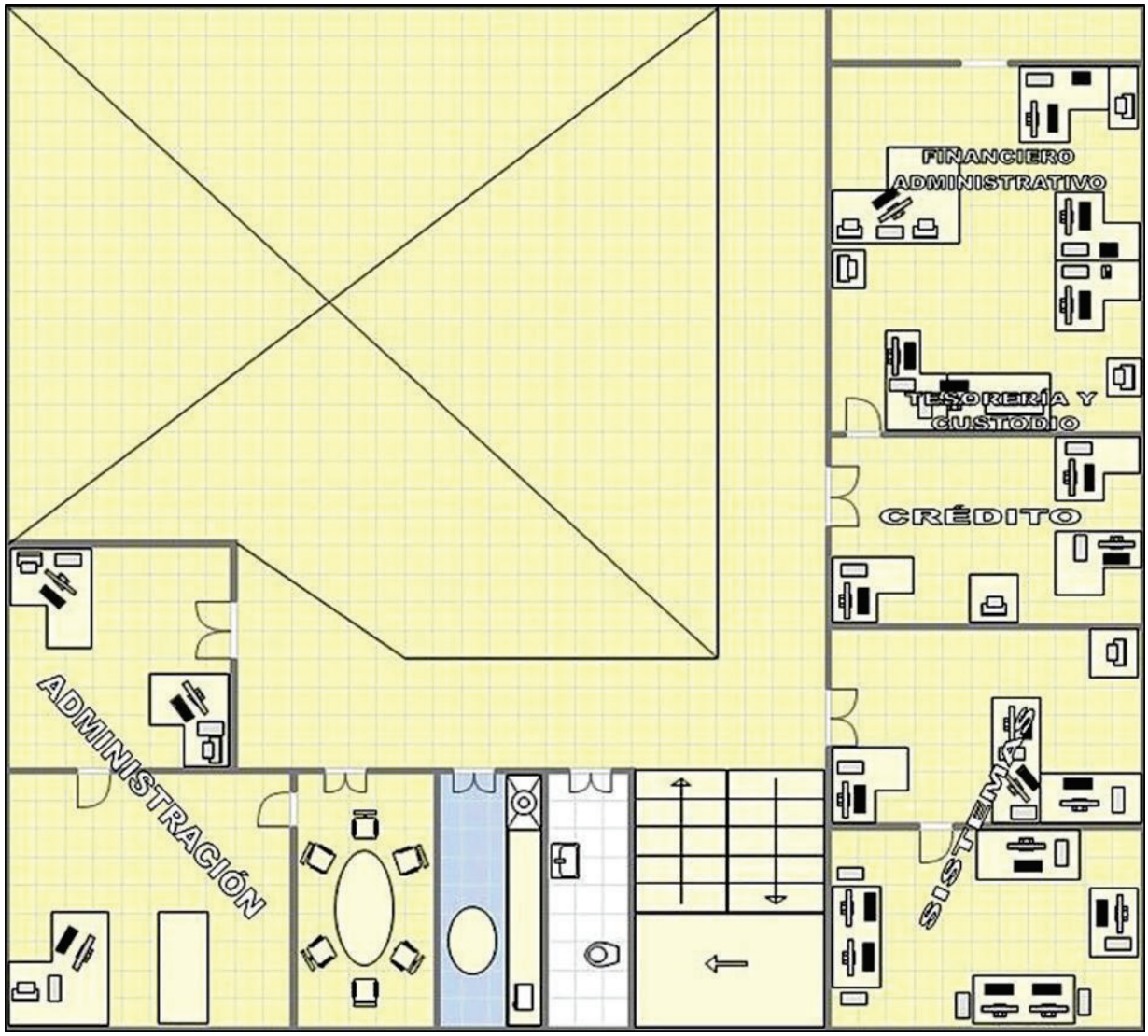

Figura 1.5 Diagrama Físico de la Organización
Elaborado por: Autores

1.1.6.1 Descripción por Departamento

El Fondo de Cesantía y Jubilación cuenta con cinco departamentos de los cuales haremos una breve descripción de cada uno de ellos.

SISTEMAS: El objetivo de este departamento es diseñar, desarrollar, implantar y mantener los sistemas de información que requiera la organización.

En este departamento trabajan dos personas:

- Jefe de Sistemas: Suarez Játiva Juan Francisco

- Asistente de Sistemas: Vásquez Yánez Ana Lucía

CRÉDITO: El objetivo de este departamento es tomar decisiones para la aprobación de créditos.

En este departamento trabajan tres personas:

- Jefe de Crédito: Villacres Procel César Manuel
- Asistente de Crédito 1: Morales Chacon Guillermo Herac
- Asistente de Crédito 2: López Villa Sylvia Rocío

FINANCIERO ADMINISTRATIVO: El objetivo de este departamento es planificar, organizar, dirigir, controlar y coordinar todas los eventos y toma de decisiones con relación al registro de las operaciones de orden económico financiero del Fondo de Cesantía y Jubilación que son susceptibles de ser expresadas en unidades monetarias, de acuerdo a las normas establecidas por los principios de contabilidad generalmente aceptados, por los servicios contralores gubernamentales y por las NIFS.

En este departamento trabajan tres personas:

- Jefe de Contabilidad: Vire Guillermo Rodrigo
- Asistente contable: Núñez Cela Verónica de los Ángeles
- Auxiliar contable: Carate Unatambo Byron Javier

TESORERÍA Y CUSTODIO: El objetivo de este departamento es garantizar de manera eficiente las actividades de custodia, control, manejo y desembolso de fondos, valores y documentos negociables que se administran en la organización.

En este departamento laboran dos personas:

- Tesorero: Castillo Guaman Willam Alfonso
- Asistente de tesorería: Toapanta Tuquerrez Mayra Florentina

ADMINISTRACIÓN: En este departamento se encuentra la secretaria la cual se encarga de apoyar a las diferentes áreas. Las funciones que realiza la secretaria es realizar oficios, memos, llamadas telefónicas, servicio al cliente.

En este departamento laboran dos personas:

- Secretaria: Lema Enríquez Andrea Salome
- Asistente de Secretaría: Guachamín Chulca Evelyn Gabriela

1.2 DEFINICIÓN DEL PROBLEMA

La información que maneja el Fondo de Cesantía y Jubilación se encuentra almacenada en el servidor central, cada cierto tiempo se sacan respaldos que son guardados en dos computadores. Adicionalmente, la información es almacenada en discos, de los cuales un disco es entregado al área de sistemas y otro es entregado en tesorería, la cual es la encargada de realizar la custodia de valores. No existe el procedimiento formal, el Fondo de Cesantía y Jubilación no cuenta con un plan de seguridad de la información que le permita gestionar de manera adecuada ese activo. Todas estas actividades se las realiza en base al conocimiento, sentido común y la experiencia lo que quiere decir que no hay nada escrito, por lo tanto, debido a que la organización maneja información crítica que es de gran valor para la misma, es necesario implantar dicho plan a fin de que mitigue los riesgos de robo, pérdida o divulgación de la información. Con el objetivo de garantizar la preservación y protección de sus datos.

1.3 DESCRIPCIÓN DEL ESTÁNDAR ISO 27000

“La ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por la ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission) que proporcionan un marco de gestión de seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.” [HYPERLINK \l "ISO" 1]

1.3.1 ORIGEN

La norma ISO/IEC 27000 aparece por primera vez en 1995 con el nombre de BS 7799 por la empresa BSI (British Standards Institution) una entidad de normalización británica, con el objetivo de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información.

A continuación se resume las distintas normas que componen la ISO 27000:

ISO/IEC 27000: Es un vocabulario estándar para el sistema de gestión de seguridad de la información y se encuentra en desarrollo actualmente.

ISO/IEC 27001: Es la certificación que deben obtener las organizaciones, es la norma que especifica los requisitos para la implantación del sistema de gestión de seguridad de la información, es la norma más importante de la familia, adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos, fue publicada como estándar internacional en octubre del 2005.

ISO/IEC 27002: Es el código de buenas prácticas para la gestión de seguridad de la información.

ISO/IEC 27003: Son directrices para la implementación de un sistema de gestión de seguridad de la información.

ISO/IEC 27004: Son métricas para la gestión de seguridad de la información, es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.

ISO/IEC 27005: Trata la gestión de riesgos de seguridad de la información, es la que proporciona recomendaciones y lineamientos de métodos, técnicas de evaluación de riesgos de seguridad en la información, en soporte de proceso de gestión de riesgos de la norma ISO 27001.

ISO/IEC 27006: Esta norma especifica los requisitos específicos para la certificación de un sistema de gestión de seguridad de la información y es usada en conjunto con

la norma 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión).

ISO/IEC 27007: Es una guía para auditar el sistema de gestión de seguridad de la información.

ISO/IEC 27799: Es una guía para implementar la ISO 27002 en la industria de la salud.

ISO/IEC 27035: Este estándar se enfoca en las actividades de detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

1.3.2 JUSTIFICACIÓN DE USO DE LOS ESTÁNDARES DE LA FAMILIA ISO/IEC 27000

Para la realización de este proyecto se hará uso de las siguientes normas que se describen a continuación:

1.3.2.1 ISO/IEC 27001 2]*}*

Esta norma proporciona directrices para la Gestión del Riesgo de Seguridad de la Información en una Organización. Sin embargo, esta norma no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información.

Por lo tanto se utilizó la Metodología de Evaluación de Riegos **MAGERIT** cuyas fases se describen en la sección 2.2.4. Es importante mencionar que dentro de esta metodología se utilizó el Anexo C de la norma ISO 27005 para la elaboración de la tabla 2.14 de evaluación del riesgo y también se utilizaron algunas cláusulas de dicha norma para describir las opciones de tratamiento del riesgo que fueron utilizadas posteriormente en la tabla 2.16 de tratamiento del riesgo.

2 ELABORACIÓN DEL PLAN DE SEGURIDAD

2.1 ANÁLISIS DE LA SEGURIDAD DE LA INFORMACIÓN EN EL FONDO DE CESANTÍA Y JUBILACIÓN DEL MDMQ

Para determinar la situación actual en lo referente a la seguridad de la información con la que cuenta el Fondo de Cesantía y Jubilación del MDMQ usaremos como punto de partida los dominios con los que cuenta la norma NTE INEN-ISO/IEC 27001. Adicionalmente se contó con el juicio experto del Ing. Juan Francisco Suarez Játiva, el cual desempeña la función de Jefe del área de sistemas en el Fondo de Cesantía y Jubilación del MDMQ.

Con la recolección de la información pertinente y de gran relevancia, a continuación en la Tabla 2.1 se ven reflejadas las observaciones en base a los dominios de la Norma ISO 27001 con los que se dispone en el Fondo de Cesantía y Jubilación del MDMQ.

DOMINIO	OBSERVACIONES
Política de seguridad	La institución no cuenta con ninguna política referente a la seguridad de la información
Aspectos organizativos de la seguridad de la información	Se está empezando a utilizar marcos referenciales como COBIT. Aun no se tiene nada hecho ni documentado.
Gestión de activos	No se cuenta con un sistema adecuado que permita manejar activos. Se utiliza hojas electrónicas para determinar la ubicación, tasa de desempeño, estado, etc.
Seguridad ligada a los recursos humanos	Se cuenta con una base de datos, en la cual están registrados los datos de los empleados, sus estudios. En otras palabras, el departamento de Recursos

	Humanos se encarga del control de empleados.
Seguridad física y ambiental	En lo referente a seguridad física se cuenta con candados, ventanas, puertas de madera. En lo referente a la seguridad ambiental, las ventanas se encuentran selladas para evitar el ingreso de polvo.
Gestión de comunicaciones y operaciones	Se cuenta con la gestión de proveedores, mantenimiento, redes, todo lo referente a comunicaciones interiores y exteriores.
Control de acceso	El acceso a los computadores está siendo controlado a través de un dominio, el cual maneja todo lo referente a políticas de acceso. Las aplicaciones se encuentran instaladas en cada computador de manera independiente. Las claves se encuentran almacenadas en una base de datos y encriptados. También se maneja todo lo referente a roles y privilegios de acceso.
Adquisición, desarrollo y mantenimiento de los sistemas de información	En si no se cuenta con un departamento propio, por lo que el área de sistemas se encarga de gestionar las tareas de adquisición, desarrollo y mantenimiento de los sistemas de información
Gestión de incidentes de seguridad de la información	Se cuenta con un pequeño manual de contingencia en caso de pérdida de información o algún desastre natural. Adicionalmente se tiene una bitácora o base de datos, en la cual se encuentran

	almacenados los incidentes más comunes y la manera de solucionarlos.
Gestión de la continuidad del negocio	Se cuenta con un plan de contingencia. Actualmente se dispone de un sistema antiguo en el que se maneja un solo servidor, por lo que si el servidor falla o pierde conexión el sistema se cae. Posteriormente se contará con un nuevo sistema en el cual se manejará un sistema de réplica en forma de espejo, con lo cual en caso de falla del servidor principal se contará con un respaldo con lo cual se garantizará la continuidad del negocio.
Cumplimiento	Actualmente se está empezando con la conformación de un plan estratégico, evaluación de rendimientos, montajes, revisiones de desempeño tanto del personal como de los sistemas.

Tabla 2.1 Situación Actual de la Seguridad de la Información
Elaborado por: Autores

En resumen, por ahora se están realizando borradores y el levantamiento de procesos de todas las operaciones. Adicionalmente se ha realizado un manual operativo de crédito. En un porcentaje aproximado se ha llegado a determinar que existe un cumplimiento del 30% a 40% con respecto a los dominios propuestos por la norma ISO 27001.

2.1.1 DISCUSIÓN DE PROBLEMAS ENCONTRADOS

A continuación se realizará una breve discusión sobre los problemas encontrados tomando como referencia cada uno de los dominios de la norma ISO 27001:

1. Política de seguridad.- Se cuenta con el respaldo necesario por parte de la Administración para la implementación de políticas que garanticen la seguridad de la información dentro y fuera de la organización pero no se cuenta con la documentación necesaria que respalde la existencia y manejo de políticas dentro de la organización.

2. Aspectos organizativos de la seguridad de la información.- La Administración ha manifestado su apoyo ante la iniciativa referente a la seguridad de la información pero dicha seguridad no es coordinada de ninguna forma con el resto de departamentos de la organización y no existe la asignación de responsabilidades correspondiente. Además, se cuenta con contratos de confidencialidad cuando la información de gran importancia es requerida por terceras partes (Municipio del Distrito Metropolitano de Quito, IESS, etc.) pero no se cuenta con asesorías ni consultorías por parte de asociaciones especializadas a nivel del Área de Sistemas.

3. Gestión de activos.- Se cuenta con un inventario de activos almacenados en una base llamada KARDEX, en el cual se maneja insumos como: implementos de oficina, materiales, etc., pero no se cuenta con un inventario de activos de información. Además no se tiene una clasificación definida de la información en el aspecto de sensibilidad e importancia de la misma.

4. Seguridad ligada a los recursos humanos.- Al momento de la contratación del personal se define el rol y las funciones que deberá cumplir el empleado pero dentro del contrato no se encuentran establecidos los lineamientos necesarios para garantizar la confidencialidad y manejo de la información antes, durante y después del empleo. Además, durante el empleo no se brinda una orientación o capacitación sobre la importancia de la seguridad de información para lograr la concientización respecto al tema dentro del personal de la organización. Respecto a las sanciones, en caso de infracciones o divulgación de información confidencial de la organización estas se ven sujetas a la legislación brindada por el Ministerio del Trabajo pero no se cuenta con políticas relacionadas a sanciones para ser aplicadas dentro de la organización.

5. Seguridad física y ambiental.- Se cuenta con controles básicos (chapas, candados, etc.) para el ingreso al área de sistemas además de que los equipos se encuentran asegurados pero no se tienen definidas seguridades más fuertes para los equipos y espacios de mayor importancia dentro de la organización. En el caso de catástrofes naturales (terremotos, incendios, inundaciones, etc.) se cuenta con los respaldos de la información de gran importancia, los cuales son almacenados en un banco que hace el papel de tesorero de dicha información pero no se cuenta con medidas adicionales. En cuanto a la protección del cableado, se ha utilizado canaletas para cubrir el cableado alrededor de la pared pero estas protecciones no son suficientes en caso de intercepción o ponchado del cable para acceder a la red y posteriormente a la información que es transmitida a través de la misma.

6. Gestión de comunicaciones y operaciones.- Se tiene un documento en el cual están descritas las normas y reglas mínimas que se deben seguir dependiendo del sistema que vaya a ser implementado o adquirido pero este documento no es suficiente como para definir los procedimientos de operación necesarios. Con respecto a las auditorias y registros de fallos, se cuenta con un archivo de control de incidencias pero no se cuenta con un registro de fallos adecuado para posteriormente ser analizados y corregidos de manera eficaz.

7. Control de acceso.- Todo lo referente a los accesos se encuentran gestionados a través de un Active Directory (AC) pero no se cuenta con la documentación necesario en la que se encuentren especificados estos aspectos de una manera clara y definida.

8. Adquisición, desarrollo y mantenimiento de los sistemas de información.- El mantenimiento de aplicaciones es realizado cuando es necesario y solo si es requerido pero no se cuenta con la documentación y lineamientos necesarios que sirvan como referencia de un tiempo prudente en el que se pueda hacer actualizaciones, revisiones o mejoras. Además, no se cuenta con ningún tipo de protección para repositorios de información. En caso de fugas de información tan solo se cuenta con logs de las bases de datos pero no se cuenta con controles que

permitan evitar situaciones en las que se comprometa información sensible e importante para la organización.

9. Gestión de incidentes de seguridad de la información.- Se han hecho análisis de riesgos, los cuales han sido notificados a la Administración pero no se han tomado las medidas correctivas necesarias. Además debido a que no se ha realizado el levantamiento y determinación de riesgos no ha sido posible determinar los responsables de gestionar oportunamente dichos riesgos. De igual manera, al no contar con la determinación de los riesgos no se tienen mecanismos necesarios para cuantificarlos, clasificarlos, etc.

10. Gestión de la continuidad del negocio.- Se tiene un plan de continuidad en caso de fallo del servidor pero físicamente si se tiene un problema con este servidor el negocio se detiene por completo debido a que no se cuenta con un soporte externo que garantice la continuidad del negocio. Además, los planes de continuidad no cuentan con la implementación de seguridad de la información, es decir tan solo son planes para mantener la continuidad del negocio.

11. Cumplimiento.- Se cuenta con estándares brindados por la Superintendencia de Bancos pero este tipo de criterios de cumplimiento no son de conocimiento del área de sistemas, es decir, no se ha profundizado en este tema. Además, se cuenta con un mantenimiento pero no se cuenta con controles necesarios para garantizar el cumplimiento técnico con el que deberían cumplir los equipos de la organización.

2.2 SELECCIÓN DE LOS ELEMENTOS A PARTIR DEL ESTÁNDAR ISO 27000

En el presente capítulo se utilizará varios elementos de las normas que han sido seleccionadas a partir del estándar ISO/IEC 27000 para continuar con el proceso de Elaboración del Plan de Seguridad de la Información del Fondo de Cesantía y Jubilación.

2.2.1 DESCRIPCIÓN DE LAS METODOLOGÍAS DE EVALUACIÓN DE RIESGOS

Existen diversas metodologías para realizar la evaluación de riesgos de los activos dentro una organización, algunas de las más importantes son: OCTAVE, NIST 800-30, RISK IT, MAGERIT. Dependiendo del área en las que vayan a ser aplicadas puede resultar conveniente utilizar una en lugar de otra.

A continuación se realizará una breve descripción de las características principales de las metodologías antes mencionadas:

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation, cuyo significado en español es: Evaluación de Amenazas, Activos y Vulnerabilidades Criticas durante la Operación) está conformado por un grupo de herramientas, técnicas y métodos definidos para la evaluación de la seguridad de la información basada en el riesgo y la planificación. El método OCTAVE es considerado un enfoque utilizado para evaluar los requerimientos de seguridad de la información en una organización. [HYPERLINK \l "CER14" 5]

OCTAVE establece que para realizar su implementación se debe formar un equipo de trabajo mixto, el cual deberá estar conformado por los jefes de cada área o departamento y los profesionales encargados de las TI dentro de la organización. La conformación de este equipo se justifica debido a que los jefes de cada área o departamento son las personas idóneas para determinar qué información es considerada delicada y la manera en la que la analizan, procesan y almacenan al cumplir con su trabajo en la organización. Por su parte, los profesionales a cargo de las TI son las personas que cuentan con los conocimientos y capacidades adecuadas para determinar el estado de la infraestructura disponible con sus respectivas fortalezas y debilidades, mediante lo cual será posible identificar los riesgos a los cuales pueden estar expuestos la información sensible y los activos críticos de la organización. 6]**}**

La NIST SP 800-30 se encuentra conformada por 9 fases, las cuales tienen por objetivo brindar un correcto análisis y evaluación de riesgos para una organización. Dichas fases son mencionadas a continuación:

1. Identificación del sistema y activos críticos.
2. Determinación de amenazas.
3. Determinación de vulnerabilidades.
4. Controles de análisis.
5. Identificación del riesgo asociado.
6. Análisis y determinación del impacto.
7. Determinación del riesgo.
8. Recomendaciones y sugerencias de control.
9. Documentación o resultado de la implementación.

Los procesos y técnicas para la evaluación de riesgos que contempla esta norma están enfocados a seguir los lineamientos y directrices establecidos en la Organización Internacional de Normalización (ISO) y la Internacional Comisión Electrotécnica Internacional (IEC). [HYPERLINK \l "Eli14" 9]

Como parte de los objetivos que contempla la NORMA SP 800-30 tenemos los siguientes:

- Aseguramiento de los sistemas de información que almacenan, procesan y transmiten información.
- Gestión de riesgos.
- Optimización de la administración de riesgos a partir del resultado en el análisis de riesgos.
- Proteger las habilidades de la organización para alcanzar su misión (no solamente relacionada a la IT, sino de toda la empresa).
- Ser una función esencial de la administración (no solo limitada a funciones técnicas de IT).

RISK IT es un marco de trabajo basado en COBIT, el cual presenta una vista comprensible de todos los riesgos relacionadas al uso de IT y un similar

Risk IT brinda una vista completa de extremo a extremo de todos los riesgos relacionados con el uso de las TI y un tratamiento similar a fondo de la gestión del riesgo, por el tono y la cultura en la parte superior, a las cuestiones operativas.

Risk IT es un marco basado en un grupo de lineamientos básicos que permiten realizar una gestión eficaz de los riesgos de TI. Este marco permite complementar a COBIT, constituyendo de esta manera un marco global que permite el control y la gestión de servicios y soluciones basados en las tecnologías impulsadas por las empresas.

Mientras COBIT proporciona un grupo de lineamientos y controles para realizar la mitigación de los riesgos de TI, RISK IT brinda un marco para que las organizaciones puedan determinar, mitigar y gestionar los riesgos relacionados con las TI. En conclusión, COBIT brinda los parámetros y lineamientos necesarios para la gestión de riesgos mientras que RISK IT brinda los extremos. 10]**}**

- **Volumen I.-** Método, constituye el volumen principal en el cual se realiza una explicación de la metodología en forma detallada.
- **Volumen II.-** Catálogo de elementos, constituye el complemento del volumen principal, el cual brinda un conjunto de inventarios útiles para la aplicación de la metodología.
- **Volumen III.-** Guía de técnicas, constituye un complemento del volumen principal, en el cual se brinda la descripción de diversas técnicas que pueden ser utilizadas durante el análisis de riesgos.

Dentro de los principales elementos con los que cuenta MAGERIT, tenemos los siguientes [HYPERLINK \l "Jor11" 13]:

- Escalas de valores cualitativos, cuantitativos y de indisponibilidad del servicio.

- Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia.
- Escala alternativa de estimación del riesgo.
- Catálogos de amenazas.
- Catálogos de medidas de control.

2.2.2 COMPARACIÓN DE LAS METODOLOGÍAS DE EVALUACIÓN DE RIESGOS

Una vez descritas las metodologías de evaluación de riesgos más importantes se procederá a realizar un cuadro comparativo teniendo en cuenta los elementos de TI a considerar y el grado en que lo hacen. Dicho cuadro comparativo fue obtenido en base a un estudio previo realizado como parte de la tesis bajo el título de: “Guía y Análisis de Gestión de Riesgos en la Adquisición e Implementación de Equipamiento y Servicios de Tecnologías de Información y Comunicaciones para Proyectos de Alcance Nacional” 14]}.

Es necesario realizar la valoración de las vulnerabilidades con la finalidad de priorizar aquellas que tienen mayor relevancia. Para lo cual, se ha realizado una adaptación de la tabla presentada en la metodología MAGERIT, en la que se ha aumentado la columna del Valor Cuantitativo a consideración de los autores de este proyecto para mejorar la comprensión de la escala de valoración.

En la tabla 2.6 se muestra la escala de valoración que se utilizó para dicho propósito en base a la probabilidad de ocurrencia con su respectiva descripción:

VALOR CUALITATIVO	VALOR CUANTITATIVO	DESCRIPCIÓN	PROBABILIDAD DE OCURRENCIA
Muy Frecuente (MF)	4	A diario	75% - 100%

Frecuente (F)	3	Una vez al mes	50% - 75%
Frecuencia Normal (FN)	2	Una vez al año	25% - 50%
Poca Frecuencia (PF)	1	Cada varios años	0% - 25%

Tabla 2.6 Valoración de Vulnerabilidades
Elaborado por: Autores

En el Anexo 2 – Apartado B y C se muestran valoradas todas las vulnerabilidades tanto lógicas como físicas, cuyos valores serán utilizados posteriormente en la tabla 2.14 de evaluación de riesgos para calcular el riesgo.

2.2.4.4 Identificación y Valoración de Impactos [HYPERLINK \l "Uni" 15]

El impacto se define como la consecuencia de la materialización de una amenaza sobre un activo. Dentro de la identificación y valoración de impactos se tomarán en cuenta determinados aspectos en función de las pérdidas técnicas que podrían generarse para la empresa u organización. A continuación, se muestran las pérdidas técnicas con sus respectivas escalas de valoración y descripciones:

a) Pérdida de confidencialidad

Escala de Valoración	Escala Cuantitativa	Descripción
Muy Bajo (MB)	1	Información relevante mínima y no sensible.
Bajo (B)	2	Información relevante mínima.
Medio (M)	3	Importante cantidad de información no sensible relevada.
Alto (A)	4	Importante cantidad de información revelada.
Muy Alto (MA)	5	Toda la información

		revelada.

Tabla 2.7 Valoración de Pérdidas Técnicas en base a la Confidencialidad
Fuente: Metodología MAGERIT
Elaborado por: Universidad Distrital Francisco José de Caldas

b) Pérdida de integridad

Escala de Valoración	Escala Cuantitativa	Descripción
Muy Bajo (MB)	1	Mínima información dañada.
Bajo (B)	2	Mínima información importante dañada.
Medio (M)	3	Gran cantidad de información dañada.
Alto (A)	4	Gran cantidad de información importante dañada.
Muy Alto (MA)	5	Toda la información destruida.

Tabla 2.8 Valoración de Pérdidas Técnicas en base a la Integridad
Fuente: Metodología MAGERIT
Elaborado por: Universidad Distrital Francisco José de Caldas

c) Pérdida de disponibilidad

Escala de Valoración	Escala Cuantitativa	Descripción
Muy Bajo (MB)	1	Mínima interrupción del servicio.
Bajo (B)	2	Mínima interrupción del servicio.
Medio (M)	3	Amplia interrupción del servicio
Alto (A)	4	Amplia interrupción de servicios primarios.
Muy Alto (MA)	5	Todos los servicios

		interrumpidos

Tabla 2.9 Valoración de Pérdidas Técnicas en base a la Disponibilidad
Fuente: Metodología MAGERIT
Elaborado por: Universidad Distrital Francisco José de Caldas

Una vez que se han determinado los valores correspondientes para el impacto en base a la integridad, confidencialidad y disponibilidad, dichos valores deben ser promediados. En caso de que el promedio resultante sea un número decimal, este será redondeado a su inmediato superior o inferior según sea el caso.

De acuerdo al valor resultante del promedio antes mencionado se procederá a calificar el posible daño que ocasionaría dicho impacto sobre los activos de la empresa u organización de acuerdo a la siguiente tabla:

IMPACTO		
Escala de Valoración	**Escala Cuantitativa**	**Descripción**
Muy Bajo (MB)	1	Daño despreciable.
Bajo (B)	2	Daño menor para la empresa u organización.
Medio (M)	3	Daño importante para la empresa u organización.
Alto (A)	4	Daño grave para la empresa u organización.
Muy Alto (MA)	5	Daño muy grave para la empresa u organización.

Tabla 2.10 Valoración del Impacto
Fuente: Metodología MAGERIT
Elaborado Por: Universidad Distrital Francisco José De Caldas

En la sección 2.2.4.6 se muestra la tabla de evaluación de riesgos en la cual se aplica cada una de las tablas mencionadas en esta sección para calcular el impacto correspondiente a cada vulnerabilidad.

2.2.4.5 Estimación del Riesgo 15]*}*

La estimación del riesgo permite determinar aquellos riesgos cuya materialización afectaría en mayor o menor porcentaje sobre los activos de una empresa u

organización. De tal manera que todos los riesgos deben ser analizados cuidadosamente mediante la aplicación de buen juicio y sentido común.

Dependiendo del nivel con el que sea catalogado el riesgo, requerirá mayor o menor atención por parte de los respectivos responsables (Gerentes, Administradores, Jefes, etc.) para lograr mitigarlos en un porcentaje aceptable que garantice que su materialización no influya sobre los activos.

Para realizar la estimación del riesgo es necesario utilizar las valoraciones tanto de las vulnerabilidades como de los impactos anteriormente efectuados, ya que ambos valores permiten determinar el valor del riesgo.

Para visualizar con mayor facilidad la representación del riesgo, es necesario aplicar una técnica matricial, la cual consiste en ubicar los niveles de las vulnerabilidades en las filas de la matriz, mientras que en las columnas se ubicarán los niveles de los impactos definidos anteriormente. A continuación, en la tabla 2.11 se muestra la respectiva matriz cualitativa que permite determinar el riesgo:

RIESGO		**VULNERABILIDAD**			
		Poco Frecuente (**PF**)	Frecuencia Normal (**FN**)	Frecuente (**F**)	Muy Frecuente (**MF**)
IMPACTO	Muy alto (**MA**)	A	MA	MA	MA
	Alto (**A**)	M	A	MA	MA
	Medio (**M**)	B	M	A	MA
	Bajo (**B**)	MB	M	M	A
	Muy Bajo (**MB**)	MB	MB	B	M

Tabla 2.11 Matriz Cualitativa para la Estimación de Riesgos
Fuente: Metodología MAGERIT
Elaborado por: Universidad Distrital Francisco José de Caldas

En la tabla 2.12 se muestra la respectiva matriz cuantitativa asociada a la matriz cualitativa anteriormente definida, en la cual el riesgo está determinado por el producto entre el impacto y la probabilidad de ocurrencia (vulnerabilidad), como se puede observar a continuación.

Por lo tanto:

*Riesgo = Impacto * Probabilidad de Ocurrencia (vulnerabilidad)*

RIESGO		VULNERABILIDAD			
		1	2	3	4
IMPACTO	5	5	10	15	20
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4

Tabla 2.12 Matriz Cuantitativa para la Estimación de Riesgos
Fuente: Metodología MAGERIT
Elaborado por: Universidad Distrital Francisco José de Caldas

Además, es necesario establecer una matriz que asocia tanto la valoración cuantitativa y cualitativa para relacionar los valores obtenidos una vez que se ha determinado el riesgo. Esto con el propósito de tomar en cuenta aquellos que tengan alta importancia y requieran de mayor atención para ser tratados. A continuación en la tabla 2.13 se muestra la respectiva matriz que permite determinar la clase riesgo:

Clase	Valoración Cualitativa	Valoración Cuantitativa
Crítico	Muy alto	10 a 20
Grave	Alto	5 a 9
Moderado	Medio	4 a 6
Despreciable	Bajo y Muy Bajo	1 a 3

Tabla 2.13 Matriz para la Clasificación de Riesgos
Fuente: Metodología MAGERIT
Elaborado por: Universidad Distrital Francisco José de Caldas

2.2.4.6 Evaluación de Riesgos

En esta sección se procederá a evaluar los riesgos en base a la metodología seleccionada, previo a eso, se realizará una breve descripción de cada una de las columnas que componen el cuadro de evaluación de riesgos. Conforme a la metodología MAGERIT se establecen los valores para las seis últimas columnas de la siguiente figura.

Nro.	Tipo de Amenaza	Nombre del Activo	Amenaza	Vulnerabilidad	Integridad	Confidencialidad	Disponibilidad	Impacto	Probabilidad de Ocurrencia	Riesgo

Figura 2.3 Cuadro de Evaluación del Riesgo
Elaborado por: Autores

Descripción:

- Nro.: Número de fila
- Tipo de Amenaza: Las amenazas se clasifican por tipos. Algunos tipos de amenazas fueron tomadas del Anexo C de la norma ISO 27005.
- Nombre del activo: Nombre del activo crítico de información.
- Amenaza: Es un evento que puede desencadenar un incidente, produciendo daños materiales o inmateriales a los activos. La lista de amenazas utilizadas se encuentran en el Anexo C de la norma ISO 27005.
- Vulnerabilidad: Las vulnerabilidades son puntos débiles que tienen los activos o grupos de activos que pueden ser aprovechadas por una amenaza. Estas vulnerabilidades fueron obtenidas en el proceso de hackeo ético y se encuentran en el Anexo 2 – Apartado B y C
- Integridad: Propiedad de proteger la exactitud y completitud de la información y cuyo valor va de 1 – 5.
- Confidencialidad: Propiedad por la cual la información no se pone a disposición de usuarios no autorizados y cuyo valor va de 1 – 5.
- Disponibilidad: Propiedad por la cual la información debe ser accesible en cualquier momento que el usuario autorizado lo requiera y cuyo valor va de 1 – 5.

- Impacto: Es la materialización de una amenaza sobre un activo. De acuerdo al criterio de los autores el impacto se determina mediante el promedio entre la integridad, confidencialidad y disponibilidad. Si el promedio resultante es un número decimal entonces aproximarlo al entero más cercano.
- Probabilidad de Ocurrencia: Es la frecuencia con la cual una vulnerabilidad puede ser aprovechada por una amenaza y cuyo valor va de 1 – 4. El listado de evaluación de vulnerabilidades se encuentran en el Anexo 2 – Apartado B y C.
- Riesgo: Se considera riesgo la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él, causando daños a la organización. El riesgo es el producto entre el impacto y la probabilidad de ocurrencia.

El cuadro de evaluación de riesgos que se presenta en la Tabla 2.14 mostrará los todos los riesgos, desde los más despreciables hasta los más críticos.

MATRIZ DE EVALUACIÓN DE RIESGOS

Nro.	Tipo de Amenaza	Nombre del Activo	Amenaza	Vulnerabilidad	Integridad	Confidencialidad	Disponibilidad	Impacto	Probabilidad de Ocurrencia	Riesgo
Evaluación del riesgo de la asociación de vulnerabilidades lógicas con las amenazas tecnológicas y humanas.										
1	Compromiso de la información	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Divulgación	Inexistencia de clasificación de la información.	5	5	5	5	4	20
2	Fallas técnicas	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Mal funcionamiento del software	Parches de software desactualizados.	4	3	5	4	3	12
3				Uso de software propietario pirateado.	4	4	3	4	3	12
4		Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Incumplimiento en el mantenimiento del sistema de información	Cuentas de usuario desactualizadas.	5	5	4	5	3	15
5				Falta de políticas para el manejo adecuado de contraseñas.	4	5	3	4	4	16
6				Falta de políticas para el manejo de backups.	5	5	5	5	4	20
7	Acciones no autorizadas	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Acceso no autorizado al sistema	Cuentas de usuario desactualizadas.	5	5	4	5	3	15
8				Falta de políticas para el manejo adecuado de contraseñas.	4	5	3	4	4	16
9		Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Corrupción y procesamiento ilegal de los datos	Inexistencia de herramientas que permitan determinar que la información enviada o receptada sea integra.	5	5	2	4	4	16
10				Inexistencia de clasificación	5	5	5	5	4	20

				de la información.						
11				Directorios de almacenamiento visibles en el escritorio.	5	5	3	4	3	12
12	Pirata informático, intruso ilegal	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Ingeniería Social	Inexistencia de clasificación de la información.	5	5	5	5	4	20
13		Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Intrusión, accesos forzados al sistema	Información de puertos abiertos.	4	4	5	4	3	12
14				Información de servicios innecesarios habilitados.	5	5	5	5	3	15
15				Información de la red interna de la organización visible.	5	4	5	5	3	15
16				Falta de monitoreo de tráfico de red en la organización.	5	5	2	4	4	16
17				Configuración del Switch por defecto.	3	3	5	4	3	12
18	Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Observar información de propietario	Inexistencia de clasificación de la información.	5	5	5	5	4	20
19				Directorios de almacenamiento visibles en el escritorio.	5	5	3	4	3	12
20				Existe más de una persona que tiene privilegios de acceso a las tecnologías de información y comunicación.	4	5	3	4	2	8
21		Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Ingreso de datos falsos o corruptos	Cuentas de usuario desactualizadas.	5	5	4	5	3	15
22				Existe más de una persona que tiene privilegios de acceso a las tecnologías de información y comunicación.	4	5	3	4	2	8

23		Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Intercepta ción	Inexistencia de herramientas que permitan determinar que la información enviada o receptada sea integra.	5	5	2	4	4	16
24		Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Código malintenci onado (virus, bomba lógica, caballo troyano)	Parches de software desactualizados.	4	3	5	4	3	12
Evaluación del riesgo de la asociación de vulnerabilidades físicas con las amenazas tecnológicas y humanas.										
25	Daño físico	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Fuego	Falta de controles, vías de escape e implementos necesarios en caso de incendio.	5	1	1	2	3	6
26				Inexistencia de alarmas en caso de alguna catástrofe.	5	1	1	2	4	8
27		Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Polvo, corrosión, congelami ento, recalenta miento.	Deficiencia en la solidez de las paredes que rodean el perímetro del área.	3	1	2	2	2	4
28				Falta de controles para sellar herméticamente las ventanas del área de sistemas.	1	3	3	2	3	6
29	Eventos Naturales	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Fenómen os sísmicos	Existe fragilidad en la infraestructura del edificio.	4	1	4	3	3	9
30				Deficiencia en la solidez de las paredes que rodean el perímetro del área.	3	1	2	2	2	4
31	Perdida de los servicios esenciales	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Falla en el sistema de suministro de agua o de aire	Inexistencia de un sistema de aire acondicionado para el área de los servidores y en general.	4	1	4	3	3	9
32				Protección insuficiente para las tomas de corriente	4	1	5	3	2	6

			acondicionado	eléctrica dentro del área.						
33		Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Pérdida de suministro de energía	Falta de suministro de energía en caso de fallo de la energía eléctrica.	3	1	5	3	3	9
34	Compromiso de la información	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Hurto de equipo	Inexistencia de cámaras de seguridad dentro del área.	4	4	1	3	4	12
35				Falta de personal de seguridad durante el día.	4	4	1	3	3	9
36				Los ordenadores no se encuentran asegurados a los puestos de trabajo.	3	3	3	3	3	9
37				Inexistencia de un registro para las personas que ingresan al área.	4	4	1	3	4	12
38				Las puertas de acceso no cuentan con la seguridad adecuada.	3	5	3	4	3	12
39				Falta de tarjetas de identificación para el personal.	2	2	1	2	3	6
40				Cajones del escritorio sin seguridades para proteger documentos y archivos sensibles y de uso cotidiano.	4	4	1	3	2	6
41				Debilidad y simplicidad de los cerrojos para cerrar las puertas mediante un candado de tamaño pequeño.	4	4	1	3	2	6
42		Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Manipulación con hardware	Los ordenadores no se encuentran asegurados a los puestos de trabajo.	3	3	3	3	3	9

43	Acciones no autorizadas	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Uso no autorizado del equipo	Falta de tarjetas de identificación para el personal.	2	2	1	2	3	6
44				Debilidad y simplicidad de los cerrojos para cerrar las puertas mediante un candado de tamaño pequeño.	4	4	1	3	2	6
45	Pirata informático, intruso ilegal	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Intrusión a áreas no autorizadas, accesos forzados al sistema	Las puertas de acceso no cuentan con la seguridad adecuada.	3	5	3	4	3	12
46				Inexistencia de un registro para las personas que ingresan al área.	4	4	1	3	4	12
47				Falta de tarjetas de identificación para el personal.	2	2	1	2	3	6
48				Falta de personal de seguridad durante el día.	4	4	1	3	3	9
49				Inexistencia de cámaras de seguridad dentro del área.	4	4	1	3	4	12
50	Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Asalto a un empleado	Falta de tarjetas de identificación para el personal.	2	2	1	2	3	6
51				Cajones del escritorio sin seguridades para proteger documentos y archivos sensibles y de uso cotidiano.	4	4	1	3	2	6

Tabla 2.14 Matriz de Evaluación del Riesgo
Elaborado por: Autores

El cuadro de evaluación de riesgos dio como resultado un total de 51 riesgos, de los cuales 28 son de nivel muy alto, 10 son de nivel alto y 13 son de nivel medio.

2.2.4.7 Manejo y Tratamiento del Riesgo [HYPERLINK \l "Uni" 15]

Una vez que se han identificado, analizado y evaluado los riesgos a los que están expuestos los activos de la organización, la Administración y los responsables de dichos activos podrán tener una visión más clara y general sobre aspectos que deben ser considerados para evitar posibles daños y perjuicios.

De tal manera que al contar con la estimación de riesgos anteriormente realizada, se podrá efectuar una evaluación general respecto a los controles y políticas que deben ser implementados para gestionar, corregir, controlar y mitigar los riesgos, garantizando de esta manera que dichos riesgos no persistan y proporcionar una mejoría considerable en el aspecto de seguridad de la información dentro de la organización.

La norma NTE INEN-ISO/IEC 27005 nos presenta diversas maneras para realizar el tratamiento de riesgos, dentro de las cuales tenemos: evitar el riesgo, reducir el riesgo, retener o aceptar el riesgo y transferir el riesgo. Para visualizarlo de mejor manera, en la Figura 2.4 se presenta la forma en que se realiza la gestión de riesgos, en la que se encuentra incluido el tratamiento de riesgos:

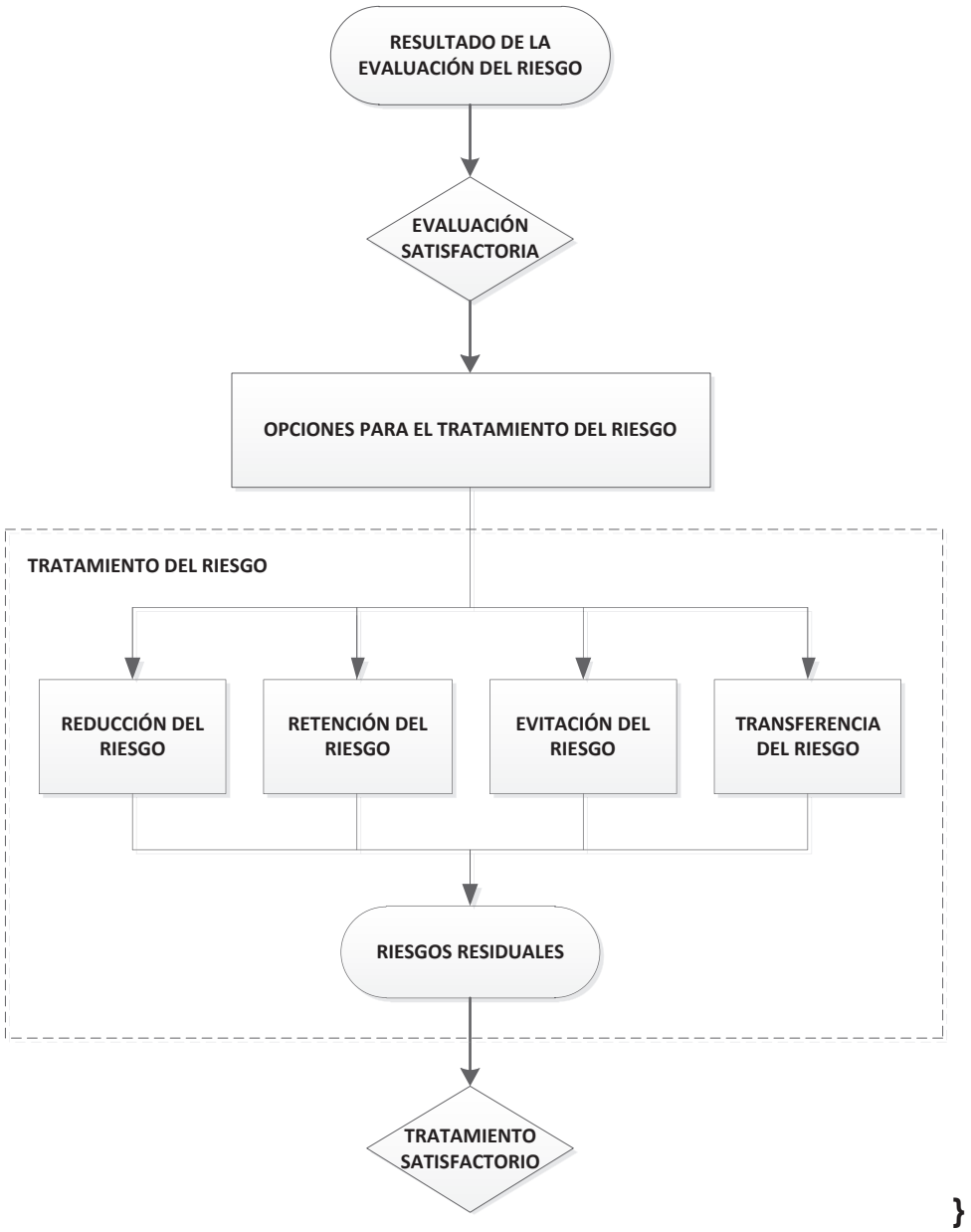

Figura 2.4 Actividades para el Tratamiento del Riesgo
Fuente: ISO/IEC FDIS 27005:2008

Previo a la definición e implementación de los controles necesarios para realizar la correspondiente gestión de riesgos; la empresa u organización debe elegir el tipo de tratamiento que se le dará a los riesgos identificados con anterioridad. A partir de la descripción de los tratamientos mencionados que nos ofrece la norma NTE INEN-ISO/IEC 27005 y la descripción de los mismos que nos ofrece la metodología MAGERIT se ha realizado una adaptación por parte de los autores de este proyecto

para obtener una definición de los tratamientos más precisa al combinar ambas descripciones. Por tal razón, a continuación en la tabla 2.15 se describen los diferentes tratamientos:

TRATAMIENTO	DESCRIPCIÓN
EVITACIÓN DEL RIESGO	Este tipo de tratamiento es considerado como la primera opción que se debe tomar en cuenta en la gestión de riesgos. Este tratamiento consiste en evitar o retirar la actividad o conjunto de actividades planificadas que generan el riesgo; o hacer cambios considerables al interior de los procesos que realiza una organización, con la finalidad de mejorar el ambiente en el que se desarrollan las mismas para evitar la generación de riesgos. (Ejemplo: controles de calidad, mantenimiento preventivo de los equipos en general, adquisición de equipos con mejor tecnología y seguridad, etc.)
REDUCCIÓN DEL RIESGO	Este tratamiento consiste en reducir el riesgo hasta su más bajo nivel para que su impacto y probabilidad de ocurrencia no sea tan grave sobre los activos de la organización. Esto se logra mediante la implementación de controles y medidas adecuadas, la optimización de los procedimientos, etc. Esta alternativa de tratamiento puede ser la de más bajo costo para la organización, ya que el riesgo al ser reducido puede ser considerado aceptable, en lugar de implementar otros controles que pueden resultar costosos e innecesarios para mitigar los riesgos. (Ejemplo: planes de contingencia, planes de continuidad del negocio, etc.)

TRANSFERENCIA DEL RIESGO	Este tratamiento consiste en transferir el riesgo total o parcialmente a una entidad externa, la cual cuenta con la experiencia necesaria y los recursos suficientes para mitigar los riesgos en caso de que se materialicen sobre los activos de la organización. Así mismo, es posible minimizar el riesgo al compartirlo con otro grupo o dependencia. (Ejemplo: contratación de pólizas de seguros, aseguradoras, etc.)
RETENCIÓN O ACEPTACIÓN DEL RIESGO	Este tratamiento consiste en que la organización se hace cargo de las consecuencias en caso de que se materialice un riesgo, el cual al ser evaluado ha dado como resultado un nivel muy bajo de incidencia sobre los activos o cuando el costo de implementación de los controles sobrepasa el valor del activo a ser protegido. Además, los riesgos residuales que se generan como consecuencia de la aplicación de controles para mitigarlos, también son aceptados por la organización.

Tabla 2.15 Tratamiento de Riesgos
Fuente: NTE INEN-ISO/IEC 27005
Elaborado por: Autores

Una vez determinados los riesgos con sus respectivos niveles de incidencia de acuerdo con los criterios anteriormente definidos en la Tabla 2.13; es necesario establecer las políticas y controles adecuados para realizar la gestión de riesgos y la gestión de seguridad correspondientes a lo largo del tiempo, con la finalidad de garantizar que los riesgos hallados no persistan dentro de la organización. La definición de políticas y controles conforman el primer paso hacia el objetivo de incrementar la seguridad de la información dentro de un ambiente tecnológico de la información.

Para realizar la gestión de riesgos correspondiente, es necesario elegir el tipo de tratamiento que se le dará a uno o varios riesgos dependiendo de su criticidad, ya que es posible combinar los diferentes tratamientos de riesgos, con la finalidad de facilitar su gestión.

Por tal razón, a los riesgos catalogados como moderados (4-6) y despreciables (1-3) se les aplicará el tratamiento de “Retención o Aceptación del Riesgo” por parte de la organización, los mismos que no se mostrarán en la tabla 2.16 pero que constan dentro del Anexo 3.

En la tabla 2.16 se visualizan los riesgos con una valoración considerable y que han sido catalogados como críticos (10 - 20) y graves (5 - 9), a los cuales se les aplicará el tratamiento de “Reducción del Riesgo”; para tal propósito, se utilizarán las políticas y controles que constan en la norma NTE INEN-ISO/IEC 27001.

Para la realización de la tabla 2.16 se tomó como base la tabla 2.14. La siguiente tabla consta de nueve columnas:

- Nro.: Número de fila
- Nombre del activo: Nombre del activo crítico de información.
- Amenaza: Es un evento que puede desencadenar un incidente, produciendo daños materiales o inmateriales a los activos. La lista de amenazas utilizadas se encuentran en el Anexo C de la norma ISO 27005.
- Vulnerabilidad: Las vulnerabilidades son puntos débiles que tienen los activos o grupos de activos que pueden ser aprovechadas por una amenaza. Estas vulnerabilidades fueron obtenidas en el proceso de hackeo ético y se encuentran en el Anexo 2 – Apartado B y C
- Impacto: Es la materialización de una amenaza sobre un activo. De acuerdo al criterio de los autores el impacto se determina mediante el promedio entre la integridad, confidencialidad y disponibilidad (Ver sección 2.2.4.6). Si el promedio resultante es un número decimal entonces aproximarlo al entero más cercano.

- Probabilidad de Ocurrencia: Es la frecuencia con la cual una vulnerabilidad puede ser aprovechada por una amenaza y cuyo valor va de 1 – 4. El listado de evaluación de vulnerabilidades se encuentran en el Anexo 2 – Apartado B y C.
- Riesgo: Se considera riesgo la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él, causando daños a la organización. El riesgo es el producto entre el impacto y la probabilidad de ocurrencia.
- Opción de Tratamiento: La opción de tratamiento de riesgo se determina mediante el valor cuantitativo del riesgo. Si el valor del riesgo es de 1-3 y de 4-6 entonces la opción de tratamiento será “Retención o Aceptación del Riesgo” y si el valor del riesgo es de 5-9 y de 10-20 entonces la opción de tratamiento será “Reducción del Riesgo”.
- Controles Seleccionados: Los controles seleccionados han sido tomados de la norma ISO 27001. A cada vulnerabilidad le corresponde de uno a varios controles dependiendo del caso, obviamente los controles seleccionados deben estar relacionados con la vulnerabilidad.

MATRIZ DE TRATAMIENTO DEL RIESGO

Nro.	Nombre del Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad de Ocurrencia	Riesgo	Opción de Tratamiento	Controles Seleccionados
Evaluación del riesgo de la asociación de vulnerabilidades lógicas con las amenazas tecnológicas y humanas.								
1	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Divulgación	Inexistencia de clasificación de la información.	5	4	20	Reducción del Riesgo	A.7.2.1 Directrices de clasificación; A.7.2.2 Etiquetado y manejo de la información.
2	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Mal funcionamiento del software	Parches de software desactualizados.	4	3	12	Reducción del Riesgo	A.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo; A.12.5.3 Restricciones a los cambios en los paquetes de software.
3			Uso de software propietario pirateado.	4	3	12	Reducción del Riesgo	A.15.1.2 Derechos de propiedad intelectual.
4	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Incumplimiento en el mantenimiento del sistema de información	Cuentas de usuario desactualizadas.	5	3	15	Reducción del Riesgo	A.11.2.1 Registro de usuario
5			Falta de políticas para el manejo adecuado de contraseñas.	4	4	16	Reducción del Riesgo	A.11.2.3 Gestión de contraseñas de usuario.
6			Falta de políticas para el manejo de backups.	5	4	20	Reducción del Riesgo	A.10.5.1 Copias de seguridad de la información; A.10.8.3 Soportes físicos en tránsito.
7	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Acceso no autorizado al sistema	Cuentas de usuario desactualizadas.	5	3	15	Reducción del Riesgo	A.11.2.1 Registro de usuario
8			Falta de políticas para el manejo adecuado de contraseñas.	4	4	16	Reducción del Riesgo	A.11.2.3 Gestión de contraseñas de usuario.
9	Sistema del Fondo	Corrupció	Inexistencia de	4	4	16	Reducció	A.10.8.1 Políticas y

	de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	n y procesam iento ilegal de los datos	herramientas que permitan determinar que la información enviada o receptada sea integra.				n del Riesgo	procedimientos de intercambio de información; A.12.3.1 Política de uso de controles criptográficos.
10			Inexistencia de clasificación de la información.	5	4	20	Reducció n del Riesgo	A.7.2.1 Directrices de clasificación; A.7.2.2 Etiquetado y manejo de la información.
11			Directorios de almacenamiento visibles en el escritorio.	4	3	12	Reducció n del Riesgo	A.11.3.2 Equipo de usuario desatendido; A.11.3.3 Política de puesto despejado y pantalla limpia.
12	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Ingeniería Social	Inexistencia de clasificación de la información.	5	4	20	Reducció n del Riesgo	A.7.2.1 Directrices de clasificación; A.7.2.2 Etiquetado y manejo de la información.
13	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Intrusión, accesos forzados al sistema	Información de puertos abiertos.	4	3	12	Reducció n del Riesgo	A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración.
14			Información de servicios innecesarios habilitados.	5	3	15	Reducció n del Riesgo	A.11.4.1 Política de uso de los servicios en red.
15			Información de la red interna de la organización visible.	5	3	15	Reducció n del Riesgo	A.11.4.3 Identificación de los equipos en las redes.
16			Falta de monitoreo de tráfico de red en la organización.	4	4	16	Reducció n del Riesgo	A.11.4.2 Autenticación de usuario para conexiones externas; A.11.4.5 Segregación de las redes; A.11.4.6 Control de la conexión a la red.
17			Configuración del Switch por defecto.	4	3	12	Reducció n del Riesgo	A.9.2.1 Emplazamiento y protección de equipos.
18	Sistema del Fondo de Jubilación (SISFJ) y Sistema	Observar informaci ón de	Inexistencia de clasificación de la información.	5	4	20	Reducció n del Riesgo	A.7.2.1 Directrices de clasificación; A.7.2.2 Etiquetado y manejo de la

	del Fondo de Cesantía (SISFC)	propietario						información.
19			Directorios de almacenamiento visibles en el escritorio.	4	3	12	Reducción del Riesgo	A.11.3.2 Equipo de usuario desatendido; A.11.3.3 Política de puesto despejado y pantalla limpia.
20			Existe más de una persona que tiene privilegios de acceso a las tecnologías de información y comunicación.	4	2	8	Reducción del Riesgo	A.11.2.2 Gestión de privilegios.
21	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Ingreso de datos falsos o corruptos	Cuentas de usuario desactualizadas.	5	3	15	Reducción del Riesgo	A.11.2.1 Registro de usuario
22			Existe más de una persona que tiene privilegios de acceso a las tecnologías de información y comunicación.	4	2	8	Reducción del Riesgo	A.11.2.2 Gestión de privilegios.
23	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Intercepta ción	Inexistencia de herramientas que permitan determinar que la información enviada o receptada sea integra.	4	4	16	Reducción del Riesgo	A.10.8.1 Políticas y procedimientos de intercambio de información; A.12.3.1 Política de uso de controles criptográficos.
24	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Código malintenci onado (virus, bomba lógica, caballo troyano)	Parches de software desactualizados.	4	3	12	Reducción del Riesgo	A.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo; A.12.5.3 Restricciones a los cambios en los paquetes de software.
Evaluación del riesgo de la asociación de vulnerabilidades físicas con las amenazas tecnológicas y humanas.								
26	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Fuego	Inexistencia de alarmas en caso de alguna catástrofe.	2	4	8	Reducción del Riesgo	A.9.1.4 Protección contra las amenazas externas y de origen ambiental.
29	Sistema del Fondo	Fenómen	Existe fragilidad en la	3	3	9	Reducció	A.9.1.4 Protección contra las

	de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	os sísmicos	infraestructura del edificio.				n del Riesgo	amenazas externas y de origen ambiental.
31	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Falla en el sistema de suministro de agua o de aire acondicionado	Inexistencia de un sistema de aire acondicionado para el área de los servidores y en general.	3	3	9	Reducción del Riesgo	A.9.1.4 Protección contra las amenazas externas y de origen ambiental.
33	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Pérdida de suministro de energía	Falta de suministro de energía en caso de fallo de la energía eléctrica.	3	3	9	Reducción del Riesgo	A.9.2.2 Instalaciones de Suministro; A.9.2.3 Seguridad del cableado.
34	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Hurto de equipo	Inexistencia de cámaras de seguridad dentro del área.	3	4	12	Reducción del Riesgo	A.9.1.1 Perímetro de seguridad física; A.9.1.3 Seguridad de oficinas, despachos e instalaciones.
35			Falta de personal de seguridad durante el día.	3	3	9	Reducción del Riesgo	A.9.1.1 Perímetro de seguridad física; A.9.1.2 Controles físicos de entrada.
36			Los ordenadores no se encuentran asegurados a los puestos de trabajo.	3	3	9	Reducción del Riesgo	A.9.2.1 Emplazamiento y protección de equipos; A.9.2.4 Mantenimiento de los equipos.
37			Inexistencia de un registro para las personas que ingresan al área.	3	4	12	Reducción del Riesgo	A.9.1.1 Perímetro de seguridad física; A.9.1.2 Controles físicos de entrada.
38			Las puertas de acceso no cuentan con la seguridad adecuada.	4	3	12	Reducción del Riesgo	A.9.1.1 Perímetro de seguridad física; A.9.1.2 Controles físicos de entrada; A.9.1.3 Seguridad de oficinas, despachos e instalaciones; A.9.1.5 Trabajo en áreas seguras.

42	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Manipulación con hardware	Los ordenadores no se encuentran asegurados a los puestos de trabajo.	3	3	9	Reducción del Riesgo	A.9.2.1 Emplazamiento y protección de equipos
45	Sistema del Fondo de Jubilación (SISFJ) y Sistema del Fondo de Cesantía (SISFC)	Intrusión a áreas no autorizadas, accesos forzados al sistema	Las puertas de acceso no cuentan con la seguridad adecuada.	4	3	12	Reducción del Riesgo	A.9.1.1 Perímetro de seguridad física; A.9.1.2 Controles físicos de entrada; A.9.1.3 Seguridad de oficinas, despachos e instalaciones; A.9.1.5 Trabajo en áreas seguras.
46			Inexistencia de un registro para las personas que ingresan al área.	3	4	12	Reducción del Riesgo	A.9.1.1 Perímetro de seguridad física; A.9.1.2 Controles físicos de entrada; A.9.1.5 Trabajo en áreas seguras.
48			Falta de personal de seguridad durante el día.	3	3	9	Reducción del Riesgo	A.9.1.1 Perímetro de seguridad física; A.9.1.2 Controles físicos de entrada.
49			Inexistencia de cámaras de seguridad dentro del área.	3	4	12	Reducción del Riesgo	A.9.1.1 Perímetro de seguridad física; A.9.1.3 Seguridad de oficinas, despachos e instalaciones.

Tabla 2.16 Matriz de Tratamiento del Riesgo
Elaborado por: Autores

2.2.4.8 Declaración de Aplicabilidad

A continuación se presentará una lista de todos los controles seleccionados en la matriz de tratamiento del riesgo en base a la norma ISO/IEC 27001, con su respectivo dominio, subdominio y objetivo de control:

Dominio	Subdominio	Objetivo	Controles	Aplica	
				Si	No
A.7 Gestión de Activos	A.7.2 Clasificación de la Información	Asegurar que la información recibe un nivel adecuado de protección	A.7.2.1 Directrices de clasificación	X	
			A.7.2.2 Etiquetado y manejo de la información	X	
A.9 Seguridad física y ambiental	A.9.1 Áreas seguras	Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización	A.9.1.1 Perímetro de seguridad física	X	
			A.9.1.2 Controles físicos de entrada	X	
			A.9.1.3 Seguridad de oficinas despachos e instalaciones	X	
			A.9.1.4 Protección contra las amenazas externas y de origen ambiental	X	
			A.9.1.5 Trabajo en áreas seguras	X	
	A.9.2 Seguridad de los equipos	Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la	A.9.2.1 Emplazamiento y protección de equipos.	X	
			A.9.2.2 Instalaciones de suministro	X	
			A.9.2.3 Seguridad del cableado	X	

		interrupción de las actividades de la organización	A.9.2.4 Mantenimiento de los equipos	X	
A.10 Gestión de comunicaciones y operaciones	A.10.5 Copias de seguridad	Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información	A.10.5.1 Copias de seguridad de la información	X	
	A.10.8 Intercambio de información	Mantener la seguridad de la información y del software intercambiado dentro de una organización y con un tercero	A.10.8.1 Políticas y procedimientos de intercambio de información	X	
			A.10.8.3 Soportes físicos en tránsito	X	
A.11 Control de acceso	A.11.2 Gestión de acceso de usuario	Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información	A.11.2.1 Registro de usuario	X	
			A.11.2.2 Gestión de privilegios	X	
			A.11.2.3 Gestión de contraseñas de usuario	X	
	A.11.3 Responsabilidades de usuario	Prevenir el acceso de usuarios no autorizados, así como evitar el que	A.11.3.2 Equipo de usuario desatendido	X	
			A.11.3.3 Política de puesto despejado y pantalla limpia	X	

		se comprometa o se produzca el robo de información o de recursos de tratamiento de la información			
	A.11.4 Control de acceso a la red	Prevenir el acceso no autorizado a los servicios en red	A.11.4.1 Política de uso de los servicios en red	X	
			A.11.4.2 Autenticación de usuario para conexiones externas	X	
			A.11.4.3 Identificación de los equipos en las redes	X	
			A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración	X	
			A.11.4.5 Segregación de las redes	X	
			A.11.4.6 Control de la conexión a la red	X	
A.12 Adquisición, desarrollo y mantenimiento de los sistemas	A.12.3 Controles criptográficos	Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos	A.12.3.1 Política de uso de controles criptográficos	X	

de información	A.12.5 Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y de la información de las aplicaciones	A.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	X	
			A.12.5.3 Restricciones a los cambios en los paquetes de software	X	
A.15 Cumplimiento	A.15.1 Cumplimiento de los requisitos legales	Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad	A.15.1.2 Derechos de propiedad intelectual	X	

Tabla 2.17 Matriz de Declaración de Aplicabilidad
Elaborado por: Autores

Debido a que el tamaño de la organización es pequeña, se considera que los controles seleccionados en la matriz de evaluación de riesgos son más que suficientes para garantizar la seguridad de los activos de información que posee el Fondo de Cesantía y Jubilación.

Estos son los controles que se utilizarán para realizar las políticas de seguridad de la información que ayudarán a la organización a reducir los riesgos a los que está expuesto el activo crítico de la misma.

2.3 ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

Para la elaboración del plan de seguridad de la información se utilizará como referencia la norma ISO 27003 la cual proporciona directrices para la implementación de un SGSI, dentro de esta norma constan un determinado número de fases con su respectivo entregable, dichas fases se describirán posteriormente para su mejor entendimiento. A continuación se describe el plan.

2.3.1 DESCRIPCIÓN DEL PLAN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El Sistema de Gestión de Seguridad de la Información cuyas abreviaturas son SGSI es el concepto base sobre el que se construye la norma ISO 27001. Para lo cual la gestión de la seguridad de la información debe hacerse a través de un proceso ordenado, documentado y conocido por toda la organización.

Un SGSI busca asegurar la integridad, confidencialidad y disponibilidad de los activos de información reduciendo los riesgos de seguridad de la información.

Es importante señalar que todas las actividades realizadas hasta esta sección pertenecen a la fase de planeación del modelo PHVA que se lo describió anteriormente en la sección 1.3.2.1.

2.3.1.1 Fases y Entregables de la Norma ISO/IEC 27003

Para el desarrollo del plan de seguridad de la información nos basaremos en la norma NTE INEN-ISO/IEC 27003:2012, la cual consta de cinco fases y cada una con sus respectivos entregables. En la figura 2.5 se muestran las fases antes mencionadas:

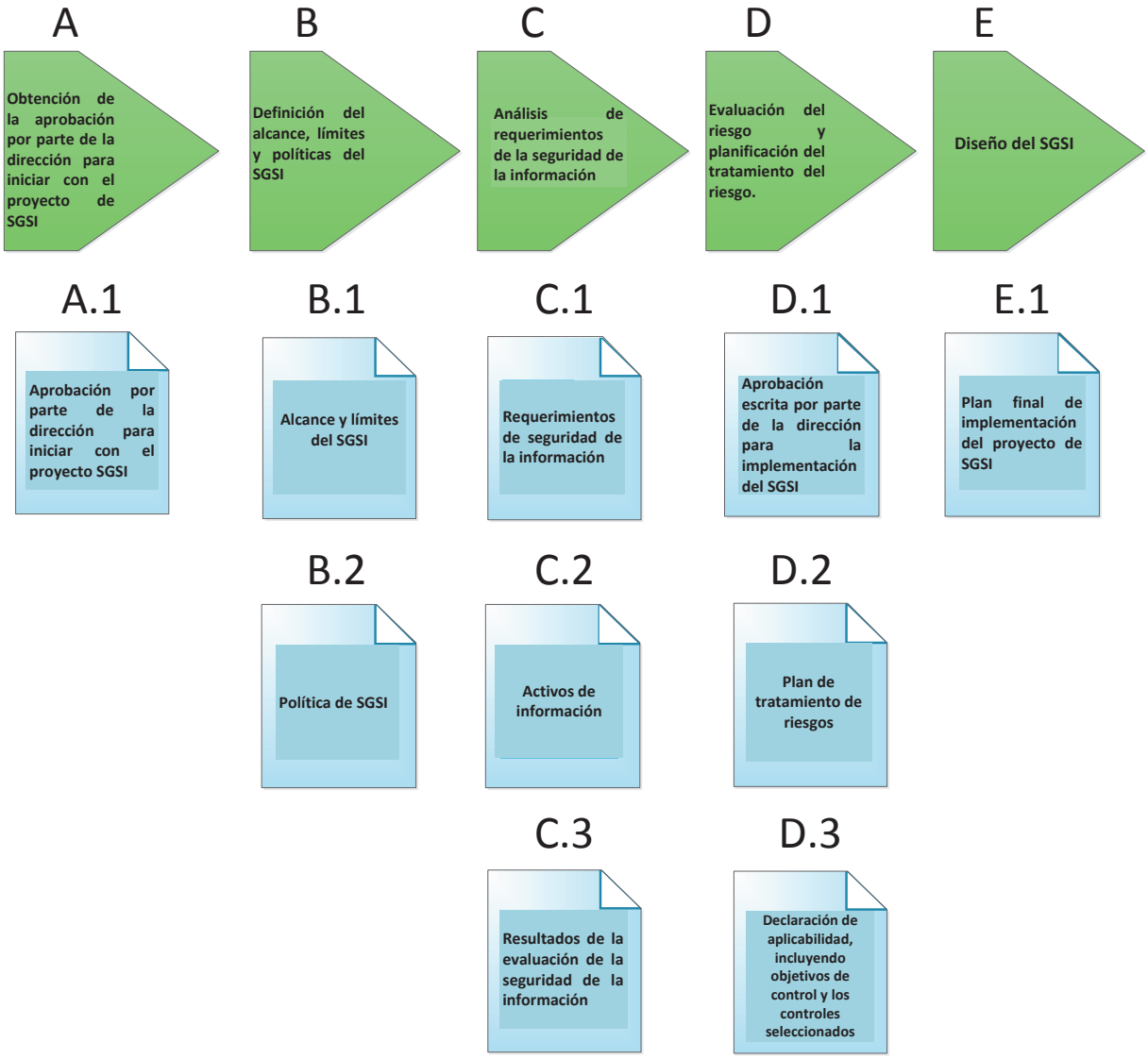

Figura 2.5 Fases del Plan de Seguridad de la Información
Fuente: ISO/IEC FDIS 27003:2012

A continuación se describen brevemente las fases del plan de seguridad de la información con sus respectivos entregables y anexos, los cuales constituyen la guía de implementación de la norma NTE INEN-ISO/IEC 27001 [16]:

A. **Obtención de la aprobación por parte de la dirección para iniciar con el proyecto de SGSI (La salida de la cláusula A (El compromiso documentado de la Dirección para planificar e implementar un SGSI) no es un requerimiento de la NTE INEN-ISO/IEC 27001).-** En esta fase el objetivo es

obtener el apoyo y compromiso de la Dirección para la implementación de un SGSI dentro de la organización. Todo esto basado en la importancia y concientización sobre el manejo de los activos y la información. El entregable correspondiente para esta fase incluye un borrador del plan del proyecto de SGSI.

A.1. Aprobación por parte de la dirección para iniciar con el proyecto de SGSI (El compromiso documentado de la Dirección para planificar e implementar un SGSI no es un requerimiento de la NTE INEN-ISO/IEC 27001).- En este punto se obtiene la aprobación preliminar y el compromiso documentado de la Dirección para iniciar el proyecto del SGSI para la organización. El documento de compromiso firmado del presente proyecto se encuentra en el Anexo 4.

B. Definición del alcance, límites y políticas SGSI (NTE INEN-ISO/IEC 27001 cláusulas 4.2.1 a) y 4.2.1 b)).- En esta fase el objetivo es definir el alcance y límites en base a tres aspectos importantes: organizacional, de las TIC y físicos. La definición de dichos alcances pueden ser aplicados a toda la organización o solo a una parte de ella. Los entregables correspondientes para esta fase incluyen la descripción del alcance y límites del SGSI y la política de SGSI.

B.1. Alcance y límites del SGSI (NTE INEN-ISO/IEC 27001 cláusula 4.2.1 a)).- en este punto se elabora un documento, en el que consta la definición de los alcances y límites para la realización del proyecto de SGSI para la organización. Un fragmento del documento elaborado se muestra a continuación:

> "*El alcance organizacional del SGSI se define en base a todos los niveles que componen la estructura organizacional del Fondo de Cesantía y Jubilación del MDMQ, teniendo en cuenta cada uno de los recursos y responsables de los departamentos.*
>
> *El SGSI estará enfocado en el Área de Sistemas que forma parte del Fondo de Cesantía y Jubilación del MDMQ, el cual deberá establecer los resguardos administrativos, técnicos y físicos, que ayudarán a la organización a protegerse de cualquier amenaza o peligro previsible que pueda afectar su*

seguridad o integridad, y que podría redundar en daños o molestias para el personal de la organización y los usuarios que hacen uso de sus servicios.

Todos los recursos pertenecientes a la organización deberán ser protegidos en base al riesgo y magnitud del daño que se podría derivar de la pérdida de información, mal uso de los recursos o acceso no autorizado a áreas restringidas."

El documento en detalle se encuentra en el Anexo 5.

B.2. Política del SGSI (NTE INEN-ISO/IEC 27001 cláusula 4.2.1 b)).- en este punto se elabora un documento, en el que constan los lineamientos adecuados para la gestión de la seguridad de la información dentro de la organización. El documento correspondiente se encuentra en el Anexo 6.

C. Análisis de requerimientos de la seguridad de la información (NTE INEN-ISO/IEC 27001 cláusulas 4.2.1.c)1) parcialmente, 4.2.1. d), 4.2.1. e)).- En esta fase el objetivo es realizar un análisis de la situación actual de la organización para determinar los requerimientos existentes y activos de información relevante que deberá ser considerada al momento de implementar el SGSI. Los entregables correspondientes para esta fase incluyen: requerimientos de seguridad de la información, activos de información y los resultados de la evaluación de la seguridad de la información.

C.1. Requerimientos de la seguridad de la información (NTE INEN-ISO/IEC 27001 cláusula 4.2.1.c)1) parcialmente).- En este punto se realiza un análisis de la situación actual de la organización, con el objetivo de determinar los requerimientos de seguridad de la información existentes en la organización. El análisis realizado se encuentra en la sección 2.1 del presente documento.

C.2. Activos de Información (NTE INEN-ISO/IEC 27001 cláusula 4.2.1. d)).- En este punto se identifican los activos de información con los que cuenta la organización, los cuales serán protegidos por el plan de seguridad de la información. La identificación de activos de información considerados como críticos, se encuentra en la sección 2.2.4.1 del presente documento.

C.3. Resultados de la evaluación de la seguridad de la información (NTE INEN-ISO/IEC 27001 cláusula 4.2.1. e)).- en este punto se realiza una evaluación preliminar sobre el estado de la seguridad de la información de la organización y las vulnerabilidades identificadas. La evaluación del riesgo será realizada posteriormente. La evaluación preliminar se encuentra en la sección 2.2.4.3 del presente documento.

D. **Evaluación del riesgo y planificación del tratamiento del riesgo (NTE INEN-ISO/IEC 27001 cláusulas 4.2.1 c) a 4.2.1 j)).-** En esta fase el objetivo es definir la metodología de evaluación de riesgos que será utilizada para determinar los controles necesarios (Ver Anexo 7). Esto ayudará en la gestión de riesgos mediante la definición del tratamiento adecuado para dichos riesgos. Los entregables correspondientes para esta fase incluyen: la aprobación escrita por parte de la Dirección para la implementación del SGSI, el plan de tratamiento de riesgos y la declaración de aplicabilidad incluyendo objetivos de control y los controles seleccionados.

D.1. Aprobación escrita por parte de la dirección para la implementación del SGSI (NTE INEN-ISO/IEC 27001 cláusulas 4.2.1. h), 4.2.1 i), 4.2.1 j)).- En este punto se debe obtener la aprobación de la Dirección para realizar la implementación SGSI, para lo cual es necesario documentar dicha aprobación. Además, en el documento debe constar la aceptación de los riesgos residuales por parte de la organización, así como la declaración de aplicabilidad. El documento de aprobación firmado por la Dirección del Fondo de Cesantía y Jubilación del MDMQ se encuentra en el Anexo 8.

D.2. Plan de tratamiento de riesgos (NTE INEN-ISO/IEC 27001 cláusulas 4.2.1 c), 4.2.1 d) 4.2.1 e), 4.2.1 f), 4.2.1 g)).- En este punto se toma en cuenta la utilización de una metodología que permita la evaluación de riesgos a los que se encuentran expuestos los activos de información de la organización. La metodología usada se encuentra descrita detalladamente con su respectiva tabla de resultados en la sección 2.2.4 del presente documento.

D.3. Declaración de aplicabilidad, incluyendo objetivos de control y los controles seleccionados (NTE INEN-ISO/IEC 27001 cláusulas 4.2.1 g), 4.2.1 j)).- En este punto es necesario realizar una lista, en la cual deberán constar los objetivos de control y los controles seleccionados para realizar el respectivo tratamiento de riesgos. En otras palabras, esta lista constituye la declaración de aplicabilidad para el presente proyecto. La declaración de aplicabilidad se encuentra en la sección 2.2.4.8 del presente documento, para más detalle ver Anexo 9.

E. Diseño del SGSI (NTE INEN-ISO/IEC 27001 cláusulas 4.2.2 a)-e), h)).- En esta fase el objetivo es completar el plan final para la implementación del SGSI. Esto comprende el diseño de la seguridad organizacional basado en las opciones de tratamiento seleccionadas para tratar los diferentes riesgos. Además se tomará en cuenta los requisitos relativos al registro y documentación, el diseño de controles y requerimientos específicos del SGSI. El entregable correspondiente para esta fase será el plan final de implementación del proyecto de SGSI.

E.1. Plan final de implementación del proyecto de SGSI (NTE INEN-ISO/IEC 27001 cláusulas 4.2.2 a)-e), h)).- en este punto se realiza el diseño detallado del plan final del proyecto de SGSI, el cual será único en su detalle para la organización específica. Dentro del diseño del plan, se ha realizado la especificación en detalle de las actividades planificadas para su implementación. La elaboración del plan final de implementación del proyecto de SGSI se encuentra detallada en el Anexo 10.

2.3.2 DESCRIPCIÓN DE LOS ENTREGABLES

Una vez obtenida la lista de controles que se utilizarán para reducir o mitigar el riesgo, se procede con la elaboración de las políticas de seguridad. Una política puede agrupar varios controles, es decir que no necesariamente se debe realizar una política para cada control.

En base a la declaración de aplicabilidad se tendrán las siguientes políticas de seguridad:

- Política de Acceso a la Red
- Política de Áreas Seguras
- Política de Creación de Backups
- Política de Cuentas Privilegiadas
- Política de Intercambio de Información
- Política de Puesto Despejado y Pantalla Limpia
- Política de Seguridad de los Equipos
- Política de Uso de Controles Criptográficos
- Política de Uso de Software Propietario
- Política y Procedimiento para el Manejo de Información Clasificada

Adicionalmente se cuenta con los siguientes entregables que forman parte de la norma ISO 27003 y que son de mucha importancia para el SGSI.

- Alcance y Límites del SGSI
- Política del SGSI
- Metodología de Evaluación de Riesgos MAGERIT
- Declaración de Aplicabilidad
- Plan de Implementación del Proyecto de SGSI
- Validación del Plan de Seguridad

La estructura de una Política de Seguridad de la Información fue realizada en base a la experiencia de los autores y al apoyo de políticas de ejemplo encontradas en la web, por lo tanto a criterio de los autores se definió la siguiente:

- Objetivo
- Alcance
- Responsables
- Documentos de Referencia
- Terminología Básica
- Desarrollo de la Política
- Validez y Gestión de Documentos

En la siguiente tabla se muestra un ejemplo de política, para ello se utilizará la Política de Puesto Despejado y Pantalla Limpia.

POLÍTICA DE PUESTO DESPEJADO Y PANTALLA LIMPIA
Objetivo El objetivo principal de este documento es establecer reglas para reducir los riesgos de acceso no autorizados, pérdida o daño de la información durante las horas normales de trabajo o fuera de ellas.
Alcance Este documento se aplica a toda información sensible sobre los puestos de trabajo del Fondo de Cesantía y Jubilación.
Responsables • **Jefe de Sistemas:** Su función es la difusión de la importancia y obligatoriedad del cumplimiento de las políticas de seguridad de información en el personal de la organización. También tiene como responsabilidad evaluar el estado de la seguridad que se brinda a la información, para tomar medidas correctivas si es necesario.
Documentos de Referencia • Norma ISO/IEC 27001, puntos A.11.3.2, A.11.3.3
Terminología Básica • **Información sensible:** es el nombre que recibe la información personal privada de un individuo, por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.
Desarrollo de la Política • Guardar documentos y dispositivos de almacenamiento (memorias) con información crítica o sensible en los cajones bajo llave. • Asegurarse de apagar o de proteger el equipo mediante la activación del

protector de pantalla con clave única de acceso, dentro y fuera del horario de trabajo. Si no es así, puede que durante la ausencia del empleado de su puesto de trabajo, otra persona consiga acceder al equipo de forma no autorizada, ocasionando daños a la información y sin dejar constancia del usuario que accedió.

- No dejar documentos a la vista, por ejemplo:
  - Nombre de Usuario y Passwords
  - Direcciones IP
  - Contratos
  - Números de Cuenta
  - Listas de Clientes
  - Propiedad Intelectual
  - Datos de Empleados
  - Cualquier cosa que no desea publicar

Retirar de manera inmediata, de las impresoras o fotocopiadoras, los documentos que contienen información sensible.

Validez y Gestión de Documentos

Este documento es válido desde el 01/02/2015 hasta 01/02/2016.

El propietario de este documento es el Administrador del Fondo de Cesantía y Jubilación, el cual, con ayuda del Jefe de Sistemas debe verificar, y si es necesario actualizar el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes relacionados con la pérdida o divulgación de información sensible.
- Cantidad de personas con acceso a puestos de trabajo no autorizadas.

Tabla 2.18 Ejemplo de Política
Elaborado por: Autores

A continuación se describe brevemente cada una de las políticas de seguridad de la información. Para ver la información completa de cada política ver el Anexo 11.

2.3.2.1 Política de Acceso a la Red

Referencia: Norma ISO/IEC 27001, puntos A.11.4.1; A.11.4.2; A.11.4.3; A.11.4.4; A.11.4.5; A.11.4.6.

El presente documento tiene por objetivo establecer las consideraciones necesarias para prevenir el acceso no autorizado a los servicios de red, bases de datos, sistemas de información, etc., por parte de terceras personas con intenciones de obtener información confidencial.

En este documento se describe la política para establecer la seguridad de acceso a la red interna de la organización, con la cual se pretende establecer el correcto manejo y acceso adecuado por parte del personal autorizado a los recursos que ofrece la misma. (Ver Anexo 11 - Política de Acceso a la Red)

2.3.2.2 Política de Áreas Seguras

Referencia: Norma ISO/IEC 27001, puntos A.9.1.1; A.9.1.2; A.9.1.3; A.9.1.4; A.9.1.5.

El presente documento tiene por objetivo establecer los requerimientos que debe cumplir la infraestructura física de la organización para garantizar la seguridad de la información y el trabajo en áreas seguras.

En este documento se describen los requerimientos que deben cumplir las áreas físicas para prevenir accesos físicos no autorizados, daños e infiltraciones en las instalaciones y substracción de información valiosa de la organización. (Ver Anexo 11 - Política de Áreas Seguras)

2.3.2.3 Política de Creación de Backups

Referencia: Norma ISO/IEC 27001, puntos A.10.5.1, A.10.8.3.

El objetivo principal de este documento es proteger y garantizar que los recursos del sistema de información (Aplicaciones y Bases de Datos) se mantengan respaldados y sean fácilmente recuperables en el momento que se necesite.

Este documento se aplica a todos los recursos utilizados para respaldar los datos del sistema de información (aplicaciones y bases de datos). (Ver Anexo 11 - Política de Creación de Backups)

2.3.2.4 Política de Cuentas Privilegiadas

Referencia: Norma ISO/IEC 27001, puntos A.11.2.1, A.11.2.2, A.11.2.3.

El objetivo principal de este documento es establecer reglas para garantizar la adecuada utilización de cuentas privilegiadas dentro del Fondo de Cesantía y Jubilación.

Este documento se aplica a todo empleado del Fondo de Cesantía el cual cuente con una cuenta privilegiada que le permita tener acceso a información sensible de la organización. (Ver Anexo 11 - Política de Cuentas Privilegiadas)

2.3.2.5 Política de Intercambio de Información

Referencia: Norma ISO/IEC 27001, puntos A.10.8.1.

El objetivo principal de este documento es asegurar el intercambio de información dentro y fuera del Fondo de Cesantía y Jubilación.

Este documento se aplica a todo tipo de información que el Fondo de Cesantía y Jubilación posea. (Ver Anexo 11 - Política de Intercambio de Información)

2.3.2.6 Política de Puesto Despejado y Pantalla Limpia

Referencia: Norma ISO/IEC 27001, puntos A.11.3.2, A.11.3.3.

El objetivo principal de este documento es establecer reglas para reducir los riesgos de acceso no autorizados, pérdida o daño de la información durante las horas normales de trabajo o fuera de ellas.

Este documento se aplica a toda información sensible sobre los puestos de trabajo del Fondo de Cesantía y Jubilación. (Ver Anexo 11 - Política de Puesto Despejado y Pantalla Limpia)

2.3.2.7 Política de Seguridad de los Equipos

Referencia: Norma ISO/IEC 27001, puntos A.9.2.1; A.9.2.2; A.9.2.3; A.9.2.4; A.12.5.2.

El presente documento tiene por objetivo establecer los requerimientos que debe cumplir la organización para garantizar la seguridad de sus equipos informáticos en caso de surgir situaciones inesperadas.

En este documento se aplica a todos los equipos tecnológicos con los cuales cuenta la organización para evitar pérdidas, daños, robos o situaciones que pongan en peligro los activos o la interrupción de las actividades de la organización. (Ver Anexo 11 - Política de Seguridad de los Equipos)

2.3.2.8 Política de Uso de Controles Criptográficos

Referencia: Norma ISO/IEC 27001, puntos A.12.3.1.

El objetivo principal de este documento es establecer controles criptográficos para la protección de la información en el Fondo de Cesantía y Jubilación.

Este documento se aplica especialmente a documentos de información digital que se envía o recibe tanto de fuentes internas como de fuentes externas al Fondo de Cesantía y Jubilación. (Ver Anexo 11 - Política de Uso de Controles Criptográficos)

2.3.2.9 Política de Uso de Software Propietario

Referencia: Norma ISO/IEC 27001, puntos A.15.1.2.

El presente documento tiene por objetivo establecer las consideraciones necesarias para el cumplimiento de los requisitos legales en cuanto al manejo de software propietario y licenciamiento con el que debe cumplir la organización.

En este documento se aplica a todo software propietario que incumpla las leyes, normativas y reglamentaciones reconocidas legalmente sobre el manejo de software propietario, licenciamiento y requerimientos de seguridad. (Ver Anexo 11 - Política de Uso de Software Propietario)

2.3.2.10 Política y Procedimiento para el Manejo de Información Clasificada

Referencia: Norma ISO/IEC 27001, puntos A.7.2.1, A.7.2.2.

El objetivo principal de este documento es garantizar que se resguarde la información en un nivel adecuado.

Este documento se aplica a todo tipo de información que el Fondo de Cesantía y Jubilación posea, ya sean estos, documentos en papel o electrónicos, bases de datos, etc. (Ver Anexo 11 - Política y Procedimiento para el Manejo de Información Clasificada)

2.4 VALIDACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

Una vez realizado el Plan de Seguridad de la información se procederá a validar el mismo, para ello se identificará un escenario y se implementará una política para dicho escenario.

2.4.1 DESCRIPCIÓN DEL ESCENARIO

El Fondo de Cesantía y Jubilación cuenta con varios departamentos que se encuentran separados por una pared sólida, la cual dificulta la comunicación entre el personal ya que no todos los puestos de trabajo cuentan con una extensión telefónica que les permita comunicarse fácilmente y que por ciertas actividades es indispensable que el personal tenga que movilizarse a otros departamentos. Esto ocasiona que los puestos y equipos de trabajo queden desatendidos por un corto o largo periodo de tiempo dependiendo de la actividad que haya ido a realizar el personal.

2.4.2 IDENTIFICACIÓN DEL ESCENARIO

Como se puede ver en la figura 2.6 el estado actual de los puestos de trabajo y equipos de la organización son bastante desatendidos.

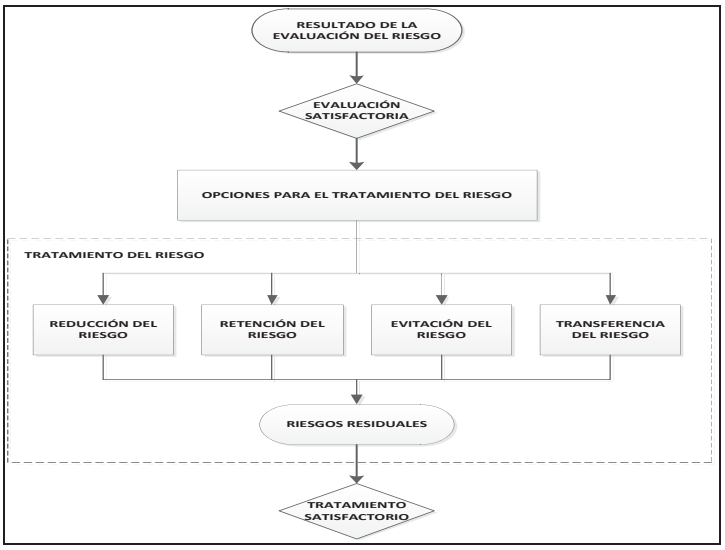

Figura 2.6 Estado de los Equipos y Puestos de Trabajo Antes de la Implementación
Fuente: Fondo de Cesantía y Jubilación

Esto se debe a que el Fondo de Cesantía y Jubilación no cuenta con políticas de seguridad de la información y por ende los funcionarios de la misma no tienen conocimiento de lo importante que es salvaguardar la información ya sea esta digital o en papel.

2.4.3 PROCEDIMIENTO DE IMPLEMENTACIÓN DE LA POLÍTICA DE PUESTO DESPEJADO Y PANTALLA LIMPIA

1. El Jefe de Sistemas es el responsable de hacer llegar el documento de Política de Puesto Despejado y Pantalla Limpia al Administrador para su respectiva aprobación. (Ver Anexo 8)
2. El Jefe de Sistemas será el responsable de dar a conocer la importancia de la seguridad de la información en la organización.
3. Una vez aprobada la política el Jefe de Sistemas es el encargado de hacer llegar o comunicar oportunamente lo que está establecido en este documento a cada uno de los miembros de la organización para su conocimiento.

   Dicho política establece que, a cada usuario que se le haya sido asignado un puesto y equipo de trabajo fijo será responsable de:

- Guardar documentos y dispositivos de almacenamiento (memorias) con información crítica o sensible en los cajones bajo llave.
- Asegurarse de apagar o de proteger el equipo mediante la activación del protector de pantalla con clave única de acceso, dentro y fuera del horario de trabajo. Si no es así, puede que durante la ausencia del empleado de su puesto de trabajo, otra persona consiga acceder al equipo de forma no autorizada, ocasionando daños a la información y sin dejar constancia del usuario que accedió.
- No dejar documentos a la vista, por ejemplo:
  - Nombre de Usuario y Passwords
  - Direcciones IP
  - Contratos
  - Números de Cuenta
  - Listas de Clientes
  - Propiedad Intelectual
  - Datos de Empleados
  - Cualquier cosa que no desea publicar
- Retirar de manera inmediata, de las impresoras o fotocopiadoras, los documentos que contienen información sensible.

4. Finalmente el Jefe de Sistemas será el encargado de evaluar el cumplimiento de dicha política y comunicar los resultados a la Administración para que se tomen las acciones correspondientes.

2.4.4 ANÁLISIS DE RESULTADOS

El Jefe de Sistemas es el encargado de dar seguimiento al cumplimiento de esta política, y por lo tanto es el responsable de evaluar los resultados obtenidos en un periodo de tiempo determinado.

Los resultados proporcionados por el Jefe de Sistemas luego de la implementación durante un mes fueron los siguientes:

Aspectos Importantes	Porcentaje de Cumplimiento
Información restringida o confidencial bajo llave.	100%
Proteger el equipo mediante la activación del protector de pantalla con clave única de acceso, dentro y fuera del horario de trabajo.	100%
Estaciones de trabajo libres de documentos, despejadas y limpias.	80%
Documentación guardada y clasificada según su importancia.	80%
Promedio:	90%

Tabla 2.19 Porcentaje de Cumplimiento de la Validación del Plan
Elaborado por: Autores

Lo cual quiere decir que el porcentaje de cumplimiento de esta política por parte de los empleados del Fondo de Cesantía y Jubilación es del 90%.

En la figura 2.7 se muestra una imagen de los resultados obtenidos luego de la implementación de la Política de Puesto Despejado y Pantalla Limpia.

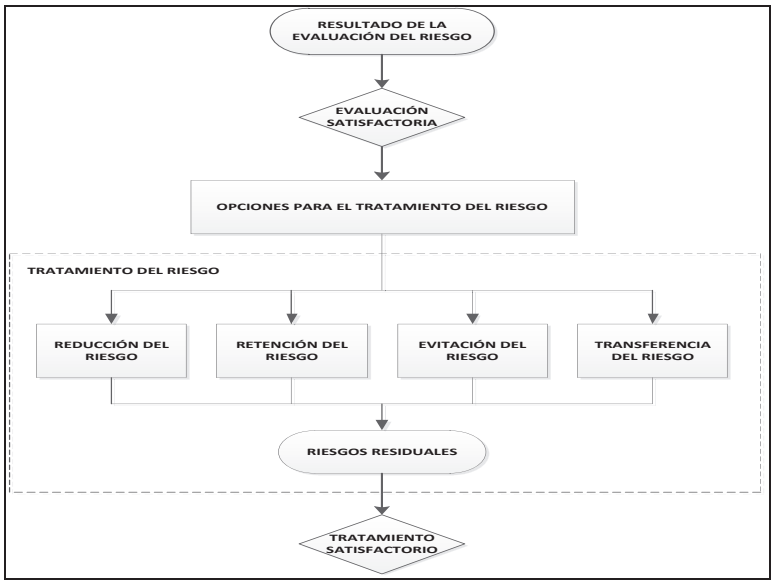

Figura 2.7 Estado de los Equipos y Puestos de Trabajo Luego de la Implementación
Fuente: Fondo de Cesantía y Jubilación

Con los resultados obtenidos se pudo determinar las siguientes conclusiones y recomendaciones.

Conclusiones

- Los funcionarios del Fondo de Cesantía y Jubilación acogieron de buena manera esta Política y la pusieron en práctica inmediatamente luego de la implementación.
- Debido al número reducido de funcionarios que trabajan en el Fondo ha sido muy fácil llegar a cada uno de ellos logrando así cambiar sus hábitos o formas de trabajo.
- El porcentaje de cumplimiento por parte del personal fue de un 90%, lo cual quiere decir que el personal ha hecho conciencia en lo importante que es preservar la información para garantizar la continuidad del negocio.
- A pesar de haber realizado el seguimiento de esta Política en un periodo de tiempo muy corto se ha podido ver grandes resultados que beneficiarán satisfactoriamente a la organización.

Recomendaciones

- Adquirir archivadores verticales u horizontales dependiendo del espacio y las necesidades del funcionario.
- Dar seguimiento a la Política constantemente de tal manera que se mantenga el porcentaje de cumplimiento actual o que supere el mismo.
- Realizar capacitaciones al personal en temas de seguridad de la información para garantizar el resguardo de la información.

Los documentos que respaldan la validación de la Política implementada dentro de la organización se encuentran en el Anexo 12.

Para más detalle de la validación del Plan de Seguridad de la Información ver Anexo 13.

3 EVALUACIÓN DE LA APLICABILIDAD DEL PLAN DE SEGURIDAD

En este punto es necesario realizar una evaluación de aplicabilidad, con lo cual se pretende justificar la implementación de los controles, políticas y procedimientos definidos dentro del plan de seguridad de la información. Para tal propósito se tomarán en cuenta ciertas restricciones y las posibles soluciones que influyen en su implementación como por ejemplo: tiempos, finanzas, técnicas, de personal, políticas e implementación de controles nuevos y existentes. También es necesario realizar un análisis de factibilidad, con el cual se pueda determinar los recursos con los que cuenta la organización y los que le hacen falta para llevar a cabo la implementación del plan de seguridad con éxito, para tal propósito se determinará la factibilidad operativa, técnica, financiera y de personal.

Además, es necesario realizar un análisis porcentual del estado de cumplimiento de los controles establecidos en la norma NTE INEN-ISO/IEC 27001 que nos permita establecer el estado actual de cumplimiento dentro de la organización y las mejoras que se pretenden obtener al implementar el plan de seguridad de la información.

3.1 JUSTIFICACIÓN DE LA APLICABILIDAD DEL PLAN DE SEGURIDAD

La justificación de aplicabilidad nos permitirá determinar el grado de influencia que tendrá la implementación del plan de seguridad de la información para un mejor manejo y protección de los activos críticos que posee la organización, así como la definición de controles y políticas que el personal correspondiente podrá usar para realizar su trabajo de manera eficaz dentro de la organización.

A continuación se realizará una comparación tomando como referencia los dominios que constan en la norma NTE INEN-ISO/IEC 27001 para determinar un porcentaje de cumplimiento actual y uno esperado. El porcentaje de cumplimiento actual estará determinado por los controles definidos dentro de cada dominio en comparación con los que cumple la organización, para lo cual tomaremos en cuenta la entrevista

realizada anteriormente y la discusión sobre los problemas encontrados, los mismos que constan en la sección 2.1 y 2.1.1 respectivamente.

Por otra parte, el porcentaje de cumplimiento esperado estará determinado por la suma de los controles ya implementados por parte de la organización más los controles considerados para su implementación que constan dentro del plan de seguridad de la información después de haberse realizado el tratamiento de riesgos, con lo cual se pretende mejorar el nivel de seguridad y resguardo de los activos críticos.

En la tabla 3.1 se muestra un ejemplo, con el cual se puede visualizar la forma en que fueron obtenidos los porcentajes de cumplimiento actual y cumplimiento esperado por cada dominio.

DOMINIO: GESTIÓN DE ACTIVOS					
No. de controles.	**Preguntas sobre el cumplimiento de los controles dentro de la organización.**	**Cumplimiento Actual**		**Cumplimiento Esperado**	
		SI (1)	**NO (0)**	**SI (1)**	**NO (0)**
1	¿Se cuenta con un inventario de activos dentro de la organización?	1		1	
2	¿Se cuenta con criterios para designar propietarios o responsables de los activos de información dentro de la organización?	1		1	
3	¿Existen reglas o políticas que permitan establecer el uso aceptable de los activos dentro de la organización?	0		0	
4	¿Existen directrices para la	0		1	

	clasificación de la información dentro de la organización?		
5	¿Existen procedimientos adecuados para el etiquetado y manejo de la información dentro de la organización?	0	1
Total de controles cumplidos		**2 / 5**	**4 / 5**
Total de controles cumplidos (%)		**40 %**	**80 %**

Tabla 3.1 Ejemplo de Obtención de Porcentajes por Dominio
Elaborado por: Autores

En la tabla 3.2 se muestra la comparación entre el porcentaje de cumplimiento actual y el porcentaje de cumplimiento esperado, en la cual se incluyen los porcentajes de todos los dominios que conforman la norma NTE INEN-ISO/IEC 27001.

DOMINIO	PORCENTAJE DE CUMPLIMIENTO ACTUAL	PORCENTAJE DE CUMPLIMIENTO ESPERADO
Política de seguridad	0 %	50 %
Aspectos organizativos de la seguridad de la información	27.27 %	27.27 %
Gestión de activos	40 %	80 %
Seguridad ligada a los recursos humanos	44,44 %	44,44 %

Seguridad física y ambiental	15,38 %	69,23 %
Gestión de comunicaciones y operaciones	21,88%	28,13%
Control de acceso	28%	60%
Adquisición, desarrollo y mantenimiento de los sistemas de información	12,5%	31,25%
Gestión de incidentes de seguridad de la información	20%	20%
Gestión de la continuidad del negocio	0%	60%
Cumplimiento	30%	40%

Tabla 3.2 Estado de Cumplimiento de la Norma NTE INEN-ISO/IEC 27001
Elaborado por: Autores

El porcentaje de cumplimiento esperado que se puede observar en la tabla 3.2, se lo logrará una vez implementado el plan de seguridad de la información en la organización. A pesar de que la organización ha implementado ciertos controles por

iniciativa propia, estos han sido tomados en cuenta nuevamente dentro del plan de seguridad de la información para ser mejorados y definidos de manera más formal.

Para alcanzar el 100% del cumplimiento en cada uno de los dominios antes mencionados, se deberán tomar en cuenta todos aquellos controles que no fueron considerados durante el tratamiento de riesgos realizado previamente. A continuación realizaremos una breve descripción de los valores de cumplimiento de cada dominio que constan en la tabla 3.2:

En el dominio A.5 Política de Seguridad se cuenta con 2 controles, razón por la cual el porcentaje de cumplimiento actual es del 0% (0 controles implementados), mientras que el porcentaje de cumplimiento esperado será del 50% (1 control será implementado), esto debido a que al contar con el apoyo por parte de la Administración y con los documentos de las políticas contempladas dentro del plan de seguridad de la información se estaría cumpliendo de manera implícita con el control A.5.1.1 Documento de Política de Seguridad de la Información. Además, cabe mencionar que este dominio se enfoca en decisiones administrativas, las cuales deberán ser discutidas una vez que se cuente con el plan de seguridad de la información para que su implementación sea exitosa dentro de la organización.

En el dominio A.6 Aspectos Organizativos de la Seguridad de la Información se cuenta con 11 controles, razón por la cual el porcentaje de cumplimiento actual y el porcentaje de cumplimiento esperado se mantienen en 27,27% (3 controles implementados), debido a que este dominio engloba temas referentes a la toma de decisiones y gestión por parte de la Administración sobre el manejo de la seguridad de la información dentro de la organización, la designación de los responsables de su correspondiente gestión y acuerdos de confidencialidad con terceros, los cuales fueron implementados por iniciativa de la organización.

En el dominio A.7 Gestión de Activos se cuenta con 5 controles, razón por la cual se puede observar un incremento considerable al pasar de un porcentaje de cumplimiento actual del 40% (2 controles implementados) a un porcentaje de cumplimiento esperado del 80% (4 controles serán implementados). Todo esto

debido a la implementación de los controles considerados dentro del plan de seguridad de la información para la organización. Dichos controles permitirán una mejor gestión y clasificación de la información importante que se maneja dentro de la organización, al igual que una mejor seguridad y protección de los activos que permiten su manipulación y procesamiento.

En el dominio A.8 Seguridad Ligada a los Recursos Humanos se cuenta con 9 controles, razón por la cual el porcentaje de cumplimiento actual y el porcentaje de cumplimiento esperado se mantienen en 44,44% (4 controles implementados), debido a que la temática que maneja este dominio se encuentra gestionada por parte del Departamento de Recursos Humanos de la organización, el mismo que conjuntamente con la Administración deberán definir los lineamientos necesarios para la contratación y el correcto manejo del personal dentro y fuera de la organización.

En el dominio A.9 Seguridad Física y Ambiental se cuenta con 13 controles; se puede observar un incremento considerable al pasar de un porcentaje de cumplimiento actual del 15,38% (2 controles implementados) a un porcentaje de cumplimiento esperado del 69,23% (9 controles serán implementados). Debido a que algunos de los controles implementados por parte de la organización son deficientes, estos han sido considerados dentro del tratamiento de riesgos, al igual que en las políticas del plan de seguridad de la información para ser mejorados. La seguridad física es un punto clave para garantizar la protección de los activos crítico con los que cuenta la organización, por lo que la implementación de los controles establecidos es primordial.

En el dominio A.10 Gestión de Comunicaciones y Operaciones se cuenta con 32 controles, razón por la cual el porcentaje de cumplimiento actual es del 21,88% (7 controles implementados) mientras que el porcentaje de cumplimiento esperado será del 28,13% (9 controles serán implementados). Los controles considerados de este dominio para ser implementados como parte del plan de seguridad de la información están enfocados a establecer un procedimiento más formal para la realización de

copias de seguridad e intercambios de información dentro de la organización y con entidades externas.

En el dominio A.11 Control de Acceso se cuenta con 25 controles, razón por la cual el porcentaje de cumplimiento actual es del 28% (7 controles implementados) mientras que el porcentaje de cumplimiento esperado será del 60% (15 controles serán implementados). Cabe mencionar que dentro de los controles tomados en cuenta de este dominio para su implementación dentro del plan de seguridad de la información también constan aquellos que fueron implementados por iniciativa propia del Departamento de Sistemas, los mismos que necesitan ser mejorados y definidos de una manera más formal. Con la implementación de estos controles se pretende mejorar la gestión de usuarios (contraseñas, privilegios, autenticación de usuarios, etc.) y determinar las responsabilidades que deben cumplir los usuarios de la organización.

En el dominio A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información se cuenta con 16 controles, razón por la cual el porcentaje de cumplimiento actual es del 12,5% (2 controles implementados) mientras que el porcentaje de cumplimiento esperado será del 31,25% (5 controles serán implementados). La implementación de los nuevos controles permitirá mejorar el tratamiento de las aplicaciones, controles criptográficos y la seguridad en los procesos de desarrollo y soporte de la organización.

En el dominio A.13 Gestión de Incidentes de Seguridad de la Información se cuenta con 5 controles, razón por la cual el porcentaje de cumplimiento actual y el porcentaje de cumplimiento esperado son del 20% (1 control implementado). Esto debido a que no se consideraron controles de este dominio dentro del plan de seguridad de la información para ser implementados. Además, este dominio hace referencia a una temática administrativa. También el personal de la organización no cuenta con la capacitación y concientización sobre la importancia de la seguridad de la información, por lo que es necesario que la Administración conjuntamente con el Departamento de Sistemas tomen las medidas pertinentes para realizar la gestión de

incidentes, las mismas que deberán ser compartidas e informadas al personal de la organización para poder contar con su colaboración.

En el dominio A.14 Gestión de la Continuidad del Negocio se cuenta con 5 controles, razón por la cual el porcentaje de cumplimiento actual es del 0% (0 controles implementados) mientras que el porcentaje de cumplimiento esperado será del 60% (3 controles serán implementados implícitamente). A pesar de que se cuenta con planes para la continuidad del negocio, estos no incluyen la temática de la seguridad de la información, por lo que no cumplen con lo requerido por los controles de este dominio. Sin embargo, los controles de este dominio no fueron considerados dentro del plan de seguridad de la información, pero una vez que se cuente con la implementación del mismo se podrá hacer la asociación correspondiente con los planes de continuidad del negocio con los que cuenta la organización para cumplir con los controles de la norma.

En el dominio A.15 Cumplimiento se cuenta con 10 controles, razón por la cual el porcentaje de cumplimiento actual es del 30% (3 controles implementados) mientras que el porcentaje de cumplimiento esperado será del 40% (4 controles serán implementados). Para este dominio se ha tomado en cuenta el control A.15.2 Derechos de Propiedad Intelectual como parte del plan de seguridad de la información para ser implementado. De esta manera se busca garantizar la legalidad de los sistemas operativos y aplicativos usados por la organización en caso de realizarse auditorías externas. Este dominio maneja la temática de cumplimiento sobre requerimientos legales, reglamentaciones y obligaciones con las que debe cumplir la organización, por lo que la Administración conjuntamente con el Departamento de Sistema deben tomar en consideración las normas y leyes con las que deben cumplir conforme con lo estipulado por las entidades regulatorias.

3.1.1 IDENTIFICACIÓN DE RESTRICCIONES PARA IMPLEMENTAR EL PLAN DE SEGURIDAD DE LA INFORMACIÓN

Existen varias restricciones que pueden impedir la implementación del Plan de Seguridad de la información entre ellos se mencionarán los siguientes:

3.1.1.1 Restricciones de Tiempo

Las restricciones de tiempo están dadas básicamente por la nueva ley, la cual establece que los fondos complementarios deben a pasar al BIESS en un periodo de tiempo indeterminado. Para este proceso hay un seguimiento minucioso por parte del Estado para que los Fondos puedan pasar lo más pronto posible al BIESS. Como la reglamentación no está clara todavía, no se sabe en qué tiempo el Fondo de Cesantía y Jubilación pase a manos del BIESS ya que el Fondo debe someterse a varias auditorias que pueden tardar varios meses o dependiendo de la complejidad pueden tardar varios años para realizar el respectivo traspaso, por lo tanto la implementación del Plan depende directamente del tiempo que el BIESS se demore en asumir el control del Fondo.

3.1.1.2 Restricciones Financieras

En cuanto a las restricciones financieras no se tiene ningún problema ya que se cuenta con un capital bastante amplio que permite invertir en la implementación del Plan de Seguridad de la Información.

3.1.1.3 Restricciones Técnicas

Las restricciones técnicas van ligadas al espacio, obviamente el espacio es uno de los factores muy importantes para tener una adecuada distribución técnica.

Una de las limitaciones que posee el Fondo de Cesantía y Jubilación es el espacio reducido en el cual se manejan los equipos, esa limitación impide que se haga una adecuada distribución del cableado, también dificulta la realización, el control y la seguridad del sistema que maneja la organización.

3.1.1.4 Restricciones de Personal

No existen restricciones para la contratación de personal especializado en el área de sistemas, pero debido a que la organización es pequeña no se puede tener un departamento completo de sistemas con un personal especializado en cada campo, razón por lo cual con dos personas a cargo del área de sistemas es más que suficiente.

3.1.1.5 Restricciones Políticas

El artículo 220 de la Ley de Seguridad Social establece que los fondos complementarios previsionales cerrados que en su origen o bajo cualquier modalidad hayan recibido aportes estatales pasarán a ser administrados por el Instituto Ecuatoriano de Seguridad Social a través de su Banco, mediante cuentas individuales. Su gestión se sujetará a los principios de seguridad, solvencia, eficiencia, rentabilidad y al control del órgano competente.

Eso implica que la actual administración del Fondo de Cesantía y Jubilación no pueda tomar ninguna acción para implementar el Plan de Seguridad de la Información ya que no se tiene conocimiento de cuando el Fondo pasará a ser administrado por el BIESS.

3.1.2 SOLUCIONES A LAS RESTRICCIONES DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

A continuación, solo se mencionarán soluciones para las restricciones existentes en el Fondo de Cesantía y Jubilación.

3.1.2.1 Soluciones de Tiempo

El traspaso del Fondo de Cesantía y Jubilación al BIESS es un hecho ya que se están realizando los procesos correspondientes para cumplir con lo establecido en la ley, una vez que esto se dé el BIESS será el encargado de tomar la decisión de mantener el fondo en sus mismas instalaciones o trasladarlas a departamentos propios del BIESS.

- Si el Fondo se mantiene en sus mismas instalaciones, el Jefe de Sistemas tiene la responsabilidad de agilitar los trámites correspondientes para la implantación del Plan de Seguridad de la Información.
- Caso contrario se debe realizar un nuevo estudio del modelo del negocio para establecer los controles correspondientes.

3.1.2.2 Soluciones Técnicas

Si el Fondo de Cesantía y Jubilación se mantiene en sus mismas instalaciones lo recomendable es hacer una redistribución de todos sus activos fijos de tal manera que el espacio sea lo suficientemente adecuado para poder dar soporte a toda la infraestructura tecnológica que posee el Fondo.

3.1.2.3 Soluciones Políticas

Realizar un nuevo análisis de tal manera que el Plan de Seguridad de la Información se ajuste a los lineamientos establecidos por el BIESS.

3.2 ANÁLISIS DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD EN EL FONDO DE CESANTÍA Y JUBILACIÓN DEL MDMQ

En el presente análisis de factibilidad se pretende dar a conocer a la Administración los recursos que serán necesarios para llevar a cabo la implementación del plan de seguridad de la información con éxito. La Administración será la encargada de aprobar la implementación del mismo en base a sus posibilidades y al grado de factibilidad con el que cuente la organización. Por lo que, para la realización del análisis de factibilidad nos basaremos en los aspectos técnicos, operacionales y económicos, los cuales se describirán a continuación:

3.2.1 FACTIBILIDAD TÉCNICA

En el análisis de factibilidad técnica se busca determinar si se cuenta con los recursos necesarios, tales como: equipos, herramientas de desarrollo, software, etc.; los mismos que permitirán que la implementación del plan de seguridad de la información sea exitosa.

En lo referente a equipos, el Fondo de Cesantía y Jubilación del MDMQ cuenta con servidores que poseen sistemas operativos Windows Server 2000, los cuales albergan a los sistemas necesarios para realizar sus correspondientes actividades dentro de la organización y por el momento han mostrado correcto funcionamiento y cuentan con sus respectivos licenciamientos.

Sin embargo, no existen equipos que puedan brindar la seguridad necesaria (cámaras de vigilancia, detectores de movimiento, etc.) para proteger los activos críticos de la organización. Además, se requieren otro tipo de equipos para mitigar los riesgos identificados previamente. Por lo que, dichos equipos son necesarios para la implementación exitosa del plan de seguridad de la información. Cabe mencionar que dichos equipos fueron considerados al tomar en cuenta la tabla 2.5 del presente documento. A continuación, en la tabla 3.3 se listan los equipos con los que debería contar la organización:

EQUIPOS	PROPÓSITO
Sistema de Alarmas	Este sistema es necesario para garantizar la seguridad dentro de la organización, con lo cual se pretende evitar percances como: robos, incendios, accesos no autorizados, etc.
Aire acondicionado	Este equipo es necesario para mantener a los servidores trabajando bajo condiciones óptimas, precautelando su integridad y evitando que sufran fallos por sobrecalentamiento.
SAI (Sistemas de Alimentación Ininterrumpida) o UPS	Este equipo será de gran utilidad en caso de que el fluido eléctrico sea interrumpido. Con dicho equipo los usuarios tendrán el tiempo necesario para guardar la información que estén generando o utilizando en ese momento, evitando que la misma se pierda por apagones inesperados de los equipos.
Cámaras de Seguridad	Estos equipos son necesarios, ya que permitirán monitorear las diversas áreas del edificio desde puntos estratégicos. Estos equipos garantizarán la seguridad del edificio en caso de suscitarse percances tales como: robos, accesos no autorizados, etc. Además brindarán la evidencia necesaria para determinar a los

	culpables y tomar las medidas correctivas adecuadas.

Tabla 3.3 Equipos Requeridos para la Implementación del Plan de Seguridad de la Información
Elaborado por: Autores

Cabe aclarar que dentro de lo que se refiere a sistemas de alarmas se incluyen otros equipos e implementos, como por ejemplo: infrarrojos para interiores, detectores de humo, sirenas, botones de pánico, etc. Además, en caso de incendios se están haciendo las gestiones necesarias para contar con el suministro de extintores y el apoyo por parte del Cuerpo de Bomberos del MDMQ.

Por lo tanto, el análisis de factibilidad técnica realizado muestra que a pesar de no contar con los equipos necesarios se están realizando todas las gestiones necesarias para la adquisición de los mismos en el menor tiempo posible. Todo esto será posible una vez superadas las restricciones de tiempo y políticas analizadas en la sección 3.1.1.

3.2.2 FACTIBILIDAD OPERACIONAL

En el análisis de factibilidad operacional u operativa se busca determinar si se cuenta con el personal capacitado y con los conocimientos necesarios para llevar a cabo la implementación del plan de seguridad de la información con éxito. Además, la factibilidad operacional pretende determinar la existencia de usuarios finales, los cuales estarán dispuestos a emplear las políticas y procedimientos generados durante la implementación del plan de seguridad de la información para la organización.

Dentro del análisis de esta factibilidad se pudo determinar que se cuenta con el apoyo por parte de la Administración para el desarrollo e implementación del plan de seguridad de la información. La Administración está consciente de la necesidad de proteger los activos críticos que posee la organización, además de establecer políticas y procedimientos que permitan mantener un mejor control y desenvolvimiento por parte del personal en las actividades realizadas dentro y fuera de la organización.

A pesar de que el personal de la organización desconoce la temática sobre seguridad de la información, es responsabilidad del Departamento de Sistema realizar la pertinente capacitación y comunicación sobre la implementación de las políticas y procedimientos establecidos dentro del plan de seguridad de la información, el cual será utilizado para dicho propósito como una guía. Además, considerando que el personal no es tan extenso (>= 15), la capacitación del mismo sería relativamente fácil asumiendo que cuentan con conocimientos básicos sobre el manejo de equipos informáticos, los cuales serán complementados con el uso de las políticas y procedimientos antes mencionados.

El Departamento de Sistemas mediante el uso del plan de seguridad de la información, deberá realizar las mejoras y adaptaciones necesarias con el objetivo de mejorar la situación de la organización en lo referente a seguridad de la información.

Por lo tanto, el análisis de factibilidad operacional realizado muestra que a pesar de no contar con todo el personal capacitado sobre el manejo de la seguridad de la información, esto podrá ser mejorado mediante la predisposición y cooperación del mismo; además de contar con la guía, capacitación y apoyo por parte del Departamento de Sistemas y la Administración.

3.2.3 FACTIBILIDAD ECONÓMICA

En el análisis de factibilidad económica se busca determinar si se cuenta con el capital necesario para realizar la implementación del plan de seguridad de la información. Mediante la realización de un análisis estimado se pretende brindar un valor referencial que posteriormente será revisado por la Administración con sus respectivas variantes dependiendo de los proveedores elegidos para solventar dichas adquisiciones.

Dentro del análisis de la factibilidad económica se tomará en consideración el costo/beneficio para la organización, tomando en cuenta que el plan de seguridad de la información no generará ingresos económicos para la misma, sino que se busca proteger los activos críticos de la organización para evitarle gasto en caso de

recuperación de información o adquisición de nuevos equipos como consecuencia de robos o daños.

Dentro del plan de seguridad de la información fueron considerados controles y políticas para precautelar la integridad de sus activos principales, los cuales son el Sistema del Fondo de Jubilación (SISFJ) y el Sistema del Fondo de Cesantía (SISFC) que se encuentran albergados en servidores de la organización de manera independiente. Además, dentro de este análisis también fueron considerados los recursos necesarios para establecer la seguridad necesaria en lo referente a accesos físicos e infraestructura del edificio. Por lo que, en la tabla 3.4 se mencionan los recursos necesarios para garantizar su integridad y seguridad, además de un valor estimado para la adquisición de los mismos:

RECURSOS REQUERIDOS	CANTIDAD	COSTO ESTIMADO UNITARIO	TOTALES
Cámaras de seguridad	7	$ 60.00	$ 420.00
Sistema de alarmas	1	$ 2.223.19	$ 2.223.19
Aire acondicionado para servidores	1	$ 915.00	$ 915.00
SAI (Sistemas de Alimentación Ininterrumpida) o UPS	6	$ 98.90	$ 593.40
Extintores para incendios	3	$ 49	$ 147

Capacitación sobre la norma NTE INEN-ISO/IEC 27001	1	$ 600	$ 600
		Valor Total	**$ 4898, 59**

Tabla 3.4 Recursos Requeridos con su Valor Estimado para la Implementación del Plan del Seguridad de la Información
Elaborado por: Autores

Cabe mencionar que dentro del sistema de alarmas se incluyen otros dispositivos (detectores de humo, infrarrojos, sirenas, botones de pánico, etc.), razón por la cual se justifica el valor considerado dentro de la tabla 3.4. Gracias a la iniciativa propia por parte de la Administración se ha logrado obtener una proforma, en la cual constan en detalle los recursos y estimados considerados por la empresa LAARCOM una vez que se ha inspeccionado el edificio en el que se desarrollan las actividades de la organización. En el Anexo 14 se encuentra la proforma detallada, más la descripción de servicios adicionales que ofrece la empresa LAARCOM para brindar la seguridad requerida.

Sin embargo, dentro de dicha proforma hace falta tomar en cuenta la implementación de ciertos dispositivos y recursos para garantizar una mejor seguridad para el activo crítico de la organización, por lo que dichos recursos faltantes han sido considerados en la tabla 3.4. Los valores estipulados en dicha tabla han sido considerados en base a un estimado de costos y funcionalidades de los equipos ofertadas por proveedores especializados en distribuir los mismos.

En lo referente a costos de capacitación, la Administración ha considerado que de ser necesario se contratará personal externo que imparta charlas y conferencias para concientizar al personal sobre la importancia de la gestión de la seguridad de la información. Sin embargo, se ha incluido el costo referencial de un curso sobre gestión de seguridades basado en la norma ISO 27001 ofrecida por el CEC (Centro de Estudios Continuos), el cual consta en la tabla 3.4. También se ha considerado la

debida capacitación en caso de emergencias, la cual se está gestionando en cooperación con el Cuerpo de Bomberos del MDMQ.

En conclusión, el capital económico necesario para la implementación del plan de seguridad de la información sería de **$4898, 59**. Se debe considerar que tan solo es un valor referencial inicial, el cual es susceptible a sufrir cambios dependiendo de la cantidad de recursos, la calidad y el tipo de proveedores que sean elegidos para sustentar las necesidades de adquisición de los mismos.

Por lo tanto, el análisis de factibilidad económica realizado muestra que la implementación del plan de seguridad de la información es viable, asumiendo que se cuenta con el software necesario y que la capacitación requerida será analizada en su momento por la Administración conjuntamente con el Departamento de Sistemas.

3.3 GUÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Plan de Seguridad de la Información se debe seguir en orden la siguiente lista de actividades. Es importante mencionar que se pueden agregar otras actividades si es que la organización lo requiere. Los responsables de la ejecución de las actividades son: el Administrador del Fondo y el Jefe de Sistemas.

1. Descripción de la empresa: Reseña histórica, Misión, Visión, Estrategias, Principios y Valores, Análisis FODA, Organigrama Estructural y Descripción del Área de TI. (Ver Secciones 1.1.1 - 1.1.6)
2. Definición del problema: Descripción de la situación actual en cuanto a la seguridad de la información. (Ver Sección 1.2)
3. Identificación de los problemas encontrados: Observaciones encontradas en base a los dominios de la norma ISO 27001. (Ver Sección 2.1)
4. Selección de la metodología de evaluación de riesgos: En este caso se ha seleccionado MAGERIT ya que cubre satisfactoriamente con los aspectos tomados en cuenta como elementos de TI y que consta de las siguientes fases. (Ver Sección 2.2.3)

4.1 Identificación del activo crítico: Selección de los activos principales que apoyan las actividades del Fondo. (Ver Sección 2.2.4.1)

4.2 Identificación de amenazas asociadas a los activos: La lista de amenazas que constan en el Anexo C de la norma ISO 27005 se asociará a los principales activos de seleccionados en el punto 4.1. (Ver Sección 2.2.4.2)

4.3 Identificación y valoración de vulnerabilidades: Descripción de vulnerabilidades lógicas y físicas con su respectiva valoración. (Ver Sección 2.2.4.3)

4.4 Identificación y valoración de impactos: MAGERIT brinda algunas matrices que permiten calcular el impacto técnico en base a la integridad, confidencialidad y disponibilidad. (Ver Sección 2.2.4.4)

4.5 Estimación del riesgo: Según MAGERIT el riesgo se obtiene mediante la multiplicación del impacto por la vulnerabilidad. (Ver Sección 2.2.4.5)

4.6 Evaluación de riesgos: Identificación de riesgos altos y muy altos en la matriz de evaluación de riesgos. (Ver Sección 2.2.4.6)

4.7 Manejo y tratamiento del riesgo: Selección de tratamiento del riesgo y establecimiento de controles. (Ver Sección 2.2.4.7)

5. Elaboración de las políticas de seguridad de la información de acuerdo a los controles establecidos. (Ver Sección 2.3)

6. Capacitación a los Empleados

7. Implementación de las Políticas de Seguridad de la información.

Una vez que el BIESS asuma el control del Fondo de Cesantía y Jubilación y apruebe que se mantenga en sus mismas instalaciones entonces se procederá inmediatamente con la implementación del Plan de Seguridad de la información.

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- El Fondo de Cesantía y Jubilación actualmente atraviesa por una grave carencia de políticas de Seguridad de la Información, lo cual conlleva a que la

organización sea vulnerable en este aspecto, siendo así y en vista de que la información es un activo de vital importancia para la empresa, se ha tomado las medidas necesarias para iniciar con el proceso de Elaboración de un Plan de Seguridad de la Información, el cual proporcionará políticas a las cuales los empleados deberán sujetarse para reducir los riesgos de pérdida, robo o divulgación de la información. Para ello se ha tomado como referencia la norma ISO 27001.

- Las técnicas de hackeo ético realizadas permitieron identificar una lista de vulnerabilidades lógicas, mientras que las vulnerabilidades físicas se las identificó mediante entrevistas al personal y principalmente en base a la percepción.
- La metodología seleccionada para la evaluación de riesgos fue MAGERIT ya que cubre todos los aspectos tomados en cuenta como elementos de TI dentro de una organización y además proporciona una lista de actividades de fácil entendimiento y muy simple de seguir. Como resultado final de aplicar esta metodología se tuvo la matriz de tratamiento del riesgo la cual permitirá proceder con la elaboración de las políticas de seguridad de la información.
- El Plan de Seguridad de la Información contiene los controles de seguridad seleccionados durante el proceso de manejo y tratamiento del riesgo, cabe recalcar que el Fondo de Cesantía y Jubilación tiene la facultad de crear nuevas políticas o modificar las que el Plan propone de acuerdo a las necesidades que en un futuro se presenten en la Organización.
- La implementación del Plan de Seguridad de la Información depende estrictamente de las restricciones de tiempo y políticas.

4.2 RECOMENDACIONES

- Se recomienda investigar e involucrar al personal de la organización sobre la importancia de implementar la seguridad de la información en las actividades que se desarrollan dentro y fuera de la organización, esto con la finalidad de mantener un correcto control sobre el manejo de los activos críticos que posee la misma.

- Se recomienda contratar los servicios de empresas expertas en el tema, con la finalidad de tener una capacitación adecuada y una visión real de la situación actual de las empresas en el país, en lo que se refiere a la gestión de la seguridad de la información.
- Se recomienda usar el sistema operativo Kali Linux, el cual es una distribución basada en Linux que contiene múltiples programas que permiten realizar pruebas de escaneo de puertos, análisis de tráfico de red, pruebas de penetración, etc., con la finalidad de determinar el nivel de seguridad con el que cuenta la organización. Sería recomendable, familiarizarse con el uso de Kali Linux y contar con la asesoría necesaria para aprender su correcto uso.
- Se recomienda la comunicación frecuente con el personal sobre situaciones o eventos ocurridos relacionados a la seguridad de la información, esto con el objetivo de obtener notificaciones, novedades y recomendaciones que serán consideradas por el Departamento de Sistema en conjunto con la Administración para ser gestionadas de manera eficaz y brindar soluciones oportunas.
- Se recomienda el uso de la metodología MAGERIT para realizar la evaluación de riesgos de la organización, ya que cubre un alto porcentaje de los elementos de TI considerados para dicha evaluación (Hardware, Software, Bases de Datos, etc.) en comparación con otras metodologías como son: OCTAVE, RISK IT, NIST 800-30. (Ver referencia [14])
- Se recomienda utilizar como base la norma NTE INEN-ISO/IEC 27001:2011, ya que cuenta con los controles necesarios para gestionar un gran número de aspectos importante referentes a la seguridad de la información. Sin embargo, es recomendable analizar otras guías como COBIT, ITIL, etc., esto con la finalidad de complementar de mejor manera la norma base.
- Se recomienda realizar la implementación del resto de controles establecidos en los dominios de la norma NTE INEN-ISO/IEC 27001:2011, esto con el objetivo de mejor aún más la seguridad de los activos críticos al considerar

aspectos adicionales. Además, esto podría contribuir para que la organización se certifique en lo referente a la seguridad de la información.

- Se recomienda crear un repositorio para que el personal de la organización pueda acceder a la documentación disponible sobre las políticas y controles, de tal manera que puedan estar informados sobre la manera de mejorar la calidad de sus actividades diarias y sobretodo contribuir con el Departamento de Sistema en el control y mejoramiento de la seguridad de la información.
- Se recomienda realizar revisiones y actualizaciones periódicas del Plan de Seguridad de la Información, ya que pueden surgir nuevas situaciones que deban ser tratadas y consideradas dentro de las políticas y controles implementados para ser mitigadas de la mejor manera posible y sin causar afectaciones a la organización.
- Se recomienda analizar diversas propuestas de proveedores de equipos y servicios de seguridad, con el objetivo de elegir la mejor y que pueda solventar las necesidades de seguridad física que requiere la organización. Además, se debe considerar la adquisición de muebles e insumos necesarios para mejor el manejo de la documentación que se genera en las actividades diarias de la organización.
- Se recomienda considerar la implementación de un sistema que permita omitir el uso de documentos impresos, evitando de esta manera que información confidencial quede expuesta sobre los escritorios y puestos de trabajo.

BIBLIOGRAFÍA

[1] (2012) ISO 27000.ES. [Online]. http://www.iso27000.es/iso27000.html

[2] Tecnología de la información, Subcomité SC 27, Técnicas de seguridad de TI. Comité Técnico ISO / IEC JTC 1. (2005) ISO. [Online]. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-1:v1:en

[3] ISOTools Excellence. (2014, Enero) SGSI. [Online]. http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

[4] ISO/IEC FDIS 27005:2008. (2008) Scribd. [Online]. https://es.scribd.com/doc/124454177/ISO-27005-espanol

[5] CERT. (2014) OCTAVE. [Online]. http://www.cert.org/resilience/products-services/octave/index.cfm

[6] Erik José Enríquez Carmona. (2013) OCTAVE, metodología para el análisis de riesgos de TI. [Online]. http://www.uv.mx/universo/535/infgral/infgral_08.html

[7] Fluidsignal Group S.A. (2007) Analisis de riesgo informatico con OCTAVE. [Online]. http://es.slideshare.net/fluidsignal/analisis-de-riesgo-informatico-con-octave

[8] Seguridad 7 "A". Metodología NIST SP 800-30. [Online]. http://seguridades7a.blogspot.com/p/nist-sp-800-30.html

[9] Elizabeth Mayora. (2014) Metodología de Gestión de Riesgo NIST 800-30. [Online]. https://prezi.com/p8moufe0ikyl/metodologia-de-gestion-de-riesgo-nist-800-30/

[10] ISACA. (2014) Risk IT Framework for Management of IT Related Business Risks. [Online]. http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx

[11] Edmundo Treviño Gelover. El Marco de Riesgo de TI. [Online]. http://www.ccisa.com.mx/InfoCCISA/Archivo/The%20Risk%20IT%20Framework.pdf

[12] Ing. Elvis Cárdenas. Metodologías para el análisis de riesgos en Seguridad Informática. [Online]. http://msnseguridad.blogspot.com/2012/08/seguridad-informatica-la-seguridad.html

[13] Jorge Esteban Eterovic and Gustavo A. Pagliari. (2011) Metodología de Análisis de Riesgos Informáticos. [Online]. http://www.cyta.com.ar/ta1001/v10n1a3.htm

[14] Jonathan Patricio Carrillo Sánchez. (2012, Agosto) Guía y Análisis de Gestión de Riesgos en la Adquisición e Implementación de Equipamiento y Servicios de Tecnologías de Información y Comunicaciones para Proyectos de Alcance Nacional. [Online]. http://bibdigital.epn.edu.ec/bitstream/15000/7866/1/CD-4557.pdf

[15] Universidad Distrital Francisco José de Caldas. Proceso de Desarrollo Open UP/OAS. [Online]. http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

[16] INEN-ISO/IEC. (2012) NTE INEN-ISO/IEC 27003.

ANEXOS

ANEXO 1 – Inventario de Activos

ANEXO 2 – Identificación y Valoración de Vulnerabilidades

ANEXO 3 – Matriz de Tratamiento del Riesgo

ANEXO 4 – Documento de Aprobación para Iniciar el Proyecto

ANEXO 5 – Alcance y Límites del SGSI

ANEXO 6 – Política del SGSI

ANEXO 7 – Metodología de Evaluación de Riesgos MAGERIT

ANEXO 8 – Documento de Aprobación para la Implementación

ANEXO 9 – Declaración de Aplicabilidad

ANEXO 10 – Plan de Implementación del Proyecto de SGS

ANEXO 11 – Directorio que contiene las siguientes Políticas y Procedimientos

- Política de Acceso a la Red
- Política de Áreas Seguras
- Política de Creación de Backups
- Política de Cuentas Privilegiadas
- Política de Intercambio de Información
- Política de Puesto Despejado y Pantalla Limpia
- Política de Seguridad de los Equipos
- Política de Uso de Controles Criptográficos
- Política de Uso de Software Propietario
- Política y Procedimiento para el Manejo de Información Clasificada

ANEXO 12 – Documentos de Validación

ANEXO 13 – Validación del Plan de Seguridad

ANEXO 14 – Propuesta de Servicios LAARCOM