UNIVERSIDAD DE EL SALVADOR

FACULTAD DE ECONOMÍA

MAESTRÍA EN CONSULTORÍA EMPRESARIAL

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA FUNDACIÓN SALVADOR DEL MUNDO DE EL SALVADOR, CON REFERENCIA AL ESTÁNDAR INTERNACIONAL ISO/IEC 27001:2005.

TRABAJO DE GRADUACIÓN PRESENTADO POR:

INGA. ADRIANA VIRGINIA FIGUEROA RIVAS

INGA. KARINA LUCÍA FLORES FIGUEROA

LICDA. SARA MIRIAM SAMAYOA RAMÍREZ

PARA OPTAR AL GRADO DE:

MAESTRA EN CONSULTORÍA EMPRESARIAL

SAN SALVADOR, EL SALVADOR, MARZO DE 2013

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

RECTOR : INGENIERO MARIO ROBERTO NIETO LOVO

SECRETARIA GENERAL : DOCTORA ANA LETICIA ZAVALETA DE AMAYA

AUTORIDADES DE LA FACULTAD DE CIENCIAS ECONÓMICAS

DECANO : MAESTRO ROGER ARMANDO ARIAS ALVARADO

VICEDECANO : MAESTRO ÁLVARO EDGARDO CALERO RODAS

SECRETARIO : INGENIERO JOSÉ CIRIACO GUTIÉRREZ

ADMINISTRADOR ACADÉMICO : LICENCIADO EDGAR ANTONIO MEDRANO

ASESOR : MAESTRO CARLOS ARMANDO PINEDA

TRIBUNAL EXAMINADOR : MAESTRO DIMAS DE JESÚS RAMÍREZ ALEMÁN

MAESTRO CARLOS ARMANDO PINEDA

DOCTOR JORGE ANIBAL CABRERA MARROQUÍN

MARZO DE 2013

SAN SALVADOR EL SALVADOR CENTRO AMÉRICA

AGRADECIMIENTOS

Agradezco infinitamente a Dios por permitirme este nuevo logro, a la Virgen María que siempre me acompaña y me guían en mi camino. A mi mamá Aminda y mis hermanos Aminda, Mario y toda mi familia que siempre me apoyaron y confiaron en mis capacidades, ya que su apoyo fue vital para alcanzar este logro profesional. A mis amigas Sarita y Kary por alcanzar esa integración de cualidades y haber trabajado en conjunto para lograr nuestra meta.

Adriana Virginia Figueroa Rivas

Gracias a Dios por sus bendiciones, por permitirme este nuevo logro y darme la oportunidad de ver una vez más sus obras en mi vida; gracias a la Virgen María que siempre me acompaña, protege e iluminan y guían mi camino. A mi familia: Lucy, Francisco, Katy y Leslie, por ser lo más valioso que Dios ha podido darme, por su amor, fortaleza y siempre estar conmigo. A mis amigas Sarita y Adri, es grandioso ver el fruto del esfuerzo, dedicación e integración de nuestras virtudes.

Karina Lucía Flores Figueroa

El más grande de mis agradecimientos al Divino niño Jesús y María Auxiliadora, por permitir que lo que inicio como un sueño se haga realidad en mi vida y cerrar este ciclo profesional con triunfo y alegría. A mi familia por el constante apoyo y especialmente a mi mamá Betty por impulsarme en mis metas, confiar siempre en mis capacidades. A mi grupo de tesis conformado por dos de mis grandes amigas a quieres admiro como seres humanos y como profesionales.

Sara Miriam Samayoa Ramírez

INDICE

INTRODUCCIÓN.

La información es un activo fundamental en las operaciones de las organizaciones; su disponibilidad, confidencialidad y seguridad son características propias de una gestión para su protección las cuales deben garantizarse para una apropiada continuidad del negocio; de este contexto, surge la iniciativa de desarrollar un Modelo de Gestión de Seguridad de la Información para la Fundación Salvador del Mundo (FUSALMO), basado en el estándar ISO/IEC 27001:2005 acerca del Sistema de Gestión de Seguridad de la Información, el cual integra las perspectivas de organización, aspectos técnicos y del recurso humano involucrado.

FUSALMO es una organización sin fines de lucro que fue fundada en el año 2001 y opera con aportes y proyectos desarrollados con aliados estratégicos; es una organización comprometida con la educación y orientación a jóvenes en grupos de riesgo, así como la integridad de la familia, entre otros. Por lo que, considerando su importancia, se hace la propuesta de un Modelo de Gestión de Seguridad de la Información acorde a sus necesidades y condiciones de operación.

En el Capítulo I, se presenta el Marco de Referencia de la investigación, indicando el planteamiento del problema, justificación, objetivos y metodología de la investigación, a fin de contextualizar el desarrollo de la misma en sus diferentes fases. Luego en el Capítulo II se establece el Marco Teórico, indicando los componentes, requerimientos y etapas del modelo.

A continuación en el Capítulo III se presenta el Diagnóstico de la Institución y en el Capítulo IV la Propuesta del Modelo de Gestión; para finalmente en el Capítulo V, presentar las Conclusiones y Recomendaciones derivadas de la investigación.

CAPÍTULO I. MARCO DE REFERENCIA

1.1 Fundación Salvador del Mundo (FUSALMO)

La Fundación Salvador del Mundo (FUSALMO) es una organización no gubernamental, sin fines de lucro, cuyo propósito le ubica como una alternativa de solución a la problemática nacional de la niñez y la juventud en condiciones de riesgo. De tal modo que, fomentando y apoyando la educación, el deporte y recreación, brinda una respuesta a las necesidades de la juventud en sus áreas de influencia.

FUSALMO nació el 17 de agosto de 2001[1], como una iniciativa de la Institución Salesiana en El Salvador, en una alianza público-privada para administrar los polideportivos construidos en zonas de riesgo y violencia juvenil, concentrándose geográficamente en las zonas de Santa Ana, San Miguel y el Municipio de Soyapango en San Salvador. Desde allí, ofrece oportunidades de desarrollo integral para la juventud salvadoreña a través de sus proyectos en los ámbitos de educación, gestión socio-laboral, prevención de la violencia, actividades deportivas, atención integral a la familia, guía pastoral, entre otros. Para el desarrollo de estos proyectos, cuenta con el apoyo de organizaciones con responsabilidad social, comprometidos con la obra desde la provisión de servicios, así como también con proyectos de auto sostenibilidad. [2]

Entre los principales destinatarios de los programas y proyectos que administra la organización están: estudiantes de centros educativos públicos, madres y padres de familia de jóvenes beneficiarios y miembros de las comunidades en los municipios de influencia.

[1] Decreto Ejecutivo No. 88 publicado en Diario Oficial de fecha 20 de Septiembre de 2001, Tomo 352.
[2] Fuente: www2.fusalmo.org

1.1.1 Filosofía Institucional[3]

a) MISION: Brindar una educación integral e innovadora con carisma salesiano a niños, niñas y jóvenes en riesgo, especialmente en los sectores de influencia de los Centros Juveniles.

b) VISION: Ser la mejor opción para niño(a) s y jóvenes en su desarrollo integral, especialmente los más necesitados, formando jóvenes realizados y agentes de cambio en su entorno social.

c) VALORES INSTITUCIONALES:

a) Amabilidad
b) Espíritu de familia
c) Apertura
d) Solidaridad
e) Testimonio
f) Transparencia
g) Eficiencia
h) Efectividad
i) Auto sostenibilidad
j) Osadía pastoral

1.1.2 Estructura Organizativa

La Institución cuenta con 98 colaboradores contratados a tiempo completo y 8 colaboradores a tiempo parcial, totalizando 106 colaboradores permanentes. Su Junta Directiva está conformada por un grupo multidisciplinario donde participan diversos sectores que colaboran y unen esfuerzos en el desarrollo de las

[3] Fuente: http://www2.fusalmo.org/index.php

actividades y programas establecidos para su misión, tal como se muestra en la tabla 1.1.

Tabla 1.1 Junta Directiva FUSALMO 2011-2014

CARGO	REPRESENTA
Presidente	Institución Salesiana
Vicepresidente	Institución Salesiana
Secretario	Asociación de Cooperadores
Pro Secretario	Asociación de Cooperadores
Tesorero	Institución Salesiana
Pro Tesorero	Institución Salesiana
Primer Vocal	Institución Salesiana
Vocal Suplente	Institución Salesiana
Segundo Vocal	FEDISAL[4]
Vocal Suplente	FEDISAL

Fuente: Informe de resultados 2011, presentación proporcionada por colaboradores de la Fundación e información disponible en el sitio web oficial de la Fundación.

Su estructura organizativa representada en forma de organigrama en la figura 1.1, presenta una distribución mixta, en la cual se observan los diferentes niveles jerárquicos. La autoridad superior está representada por la Asamblea General, seguido de la Junta Directiva.

Luego se encuentra la Dirección Ejecutiva, de la cual dependen componentes críticos en la organización: Gestión y diseño de proyectos, el Consejo Ejecutivo, Recursos Humanos y Comunicaciones. Luego se ubican la Dirección del Oratorio (El comité pastoral ejerce autoridad sobre la misma) y las gerencias técnicas, administrativas y financieras.

[4] Fundación para la Educación Integral Salvadoreña (FEDISAL)

Organigrama general de FUSALMO

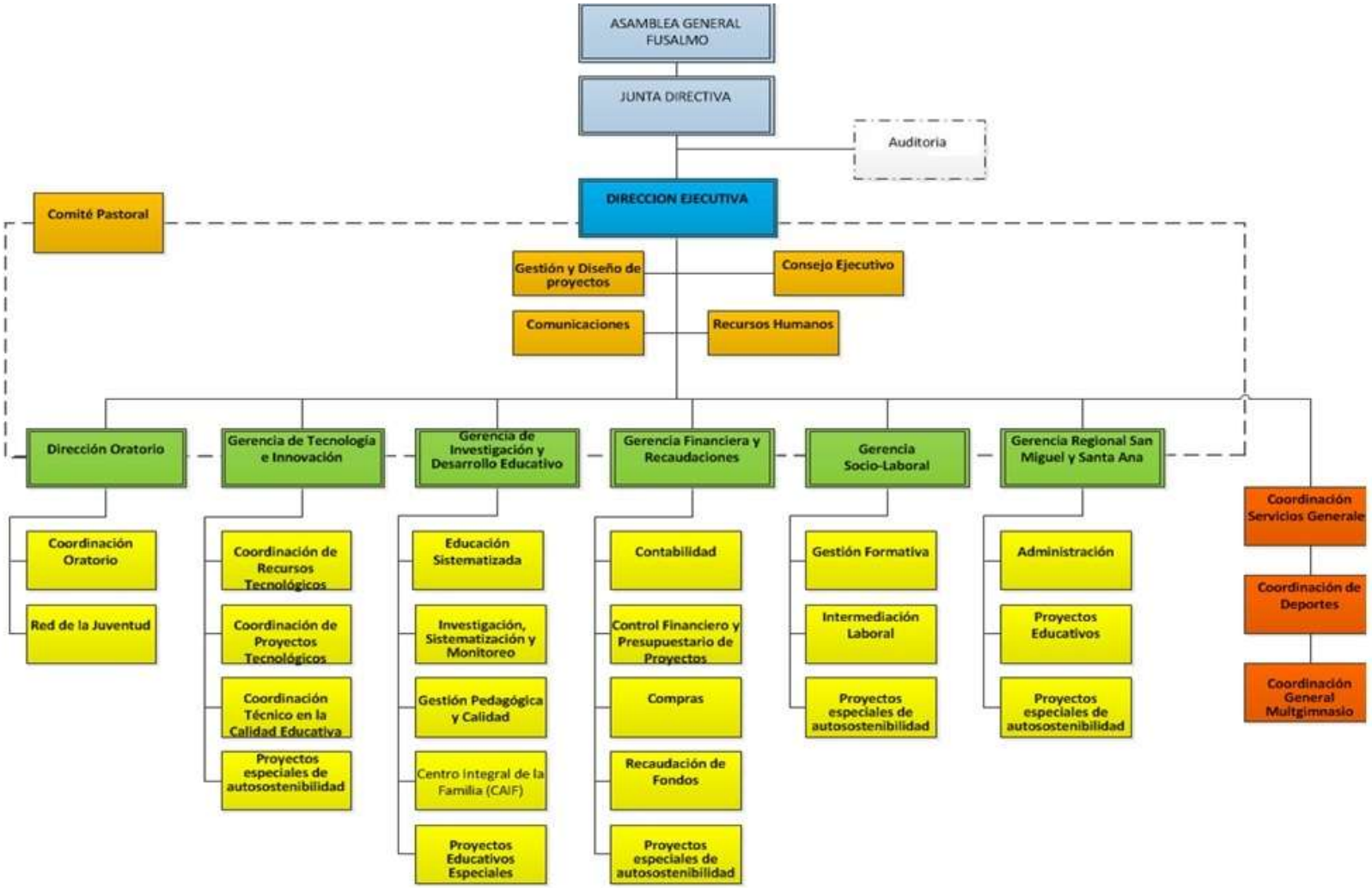


Figura 1.1 Organigrama Institucional de FUSALMO

1.2. Planteamiento del Problema

FUSALMO, siendo una organización que brinda servicios de apoyo a la juventud en diferentes ámbitos y muy especialmente en el campo educativo, actualmente carece de un Sistema de Gestión de Seguridad de la Información que garantice la preservación de la misma, su seguridad y confidencialidad.

En el pasado, esta situación ya le ha representado costos directos e indirectos en cuanto a pérdida de información y vulnerabilidades en seguridad y confidencialidad, dado que no se cuenta con un enfoque a procesos, ni un manual de políticas de seguridad de la información que a su vez permita la gestión de riesgos, generar mayor confianza y credibilidad ante sus destinatarios, clientes y aliados estratégicos.

1.2.1 Preguntas de investigación

a) ¿Existen mecanismos de control de seguridad para el acceso a la información?
b) ¿Existe una política de seguridad de la información aceptada institucionalmente?
c) ¿Qué beneficios propiciaría para la fundación la implementación de un sistema de gestión de seguridad de la información?
d) ¿La unidad que gestiona los sistemas de información cuenta con procesos documentados?
e) ¿La institución cuenta con las instalaciones físicas y tecnológicas apropiadas para garantizar la seguridad de la información?
f) ¿La elaboración de un sistema de gestión de seguridad de la información basado en procesos contribuirá a la gestión de la seguridad de la información?
g) ¿La política actual de seguridad de la información incorpora la filosofía institucional?

1.2.2 Definición del problema

¿Un modelo de gestión de seguridad de la información para FUSALMO minimizaría los riesgos de pérdida de la misma, en aras de alcanzar los objetivos y metas de la Institución?

1.3 Justificación

Actualmente la información representa un bien de gran valor, para la Institución en estudio es clave desde la planificación y ejecución de proyectos educativos y sociales, así como en sus relaciones con colaboradores estratégicos y entidades del sector productivo, donde estos últimos cuentan con procesos estandarizados y certificados internacionalmente; por tanto la disponibilidad, confidencialidad e integridad de la información son objetivos clave para la administración.

Este esfuerzo de la Institución, aporta mayor respaldo y confianza en las relaciones con sus colaboradores, así como una muestra voluntaria de mejora continua y compromiso con la razón de ser de la misma.

Adicionalmente, el desarrollo de un modelo de gestión de seguridad de la información permitirá:

a) Conocer los riesgos y poder gestionarlos.
b) Implementar controles que minimicen los riesgos y amenazas en seguridad de la información.
c) Lograr mayor credibilidad, confianza y fiabilidad ante sus destinatarios y aliados estratégicos
d) Mejora en las relaciones con clientes y aliados estratégicos.
e) Mayor nivel de compromiso de parte de sus colaboradores
f) Operaciones basadas en procesos.
g) Adopción de mejores prácticas de la industria.

h) Procesos que garanticen la seguridad, confidencialidad e integridad de la información.
i) Mayor reconocimiento y prestigio en el sector.

A sus aliados estratégicos:

a) Compromiso con la mejora continua
b) Entorno de trabajo basado en procesos y compatible con otros modelos de gestión aplicados a la industria y demás sectores productivos.
c) Desarrollo de procesos que garanticen la confidencialidad, seguridad e integridad de la información.

A sus destinatarios:

a) Mejora continua en los servicios prestados, evitando uso inadecuado de la información.
b) Consolidación del equipo de trabajo dentro de la organización y su identidad institucional.
c) Procesos que garanticen la seguridad, confidencialidad e integridad de la información.
d) Mayor respaldo y compromiso en las relaciones con los aliados estratégicos y el proyecto institucional.
e) Apertura de nuevos proyectos y la prolongación de los ya vigentes de acuerdo al ciclo de vida de los mismos.

1.4 Cobertura

1.4.1 Temporal

Tomando en cuenta que la Institución cuenta con gran trayectoria en el desarrollo de proyectos, consolidando sus inicios en el campo educativo alrededor del año 2003 y que desde entonces ha evolucionado continuamente, así como también en el campo de la tecnología y las comunicaciones; para propósitos de la

investigación se consideró objeto de estudio la información de los últimos cinco años, comprendidos del año 2007 a 2011 en relación a la regulación, administración y seguridad de la información de acuerdo a su relevancia, así como los documentos actualizados relacionados con la filosofía de la organización.

1.4.2 Geográfica

El estudio se realizó en la Fundación Salvador del Mundo (FUSALMO) de El Salvador contemplando sus sedes en Soyapango, San Miguel y Santa Ana; trabajando así conjuntamente con la sede central ubicada en Soyapango sobre la intersección carretera a San Miguel y calle a Tonacatepeque, después del paso a desnivel de Unicentro Soyapango. Estadio “Plaza España”.

1.5 Alcance y limitaciones

La investigación comprendió el establecimiento del Modelo de gestión de seguridad de la información para la Institución, el cual contempla la realización del diagnóstico de la misma en cuanto a sus procesos, organización y prácticas en seguridad de la información bajo el enfoque de requerimientos del estándar internacional, además el establecimiento de una metodología y resultados de análisis de riesgos, elaboración del manual de políticas de seguridad de la información, plan de implementación del sistema y recomendaciones.

Entre las limitantes del proceso figuran la no documentación de los procesos de la Institución en un Manual de Procedimientos, a pesar de que algunos de estos son ejecutados en la práctica y se dispone de evidencias de su desarrollo; así como los requerimientos de confidencialidad por parte de la Institución a fin de la no divulgación de información crítica, permitiendo el acceso a la misma para verificación y restringiendo su publicación en la documentación del proceso

1.6 Objetivos

1.6.1 Objetivo General

Elaborar propuesta de modelo de gestión de seguridad de la información para la Fundación Salvador del Mundo de El Salvador, de acuerdo al estándar internacional ISO/IEC 27001:2005.

1.6.2 Objetivos Específicos

a) Realizar un diagnóstico de la situación actual de la Institución en relación a la seguridad de la información, de acuerdo a los requerimientos del estándar ISO/IEC 27001:2005.
b) Definir aspectos de mejora para la posterior implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en relación a los requerimientos del estándar ISO/IEC 27001:2005.
c) Desarrollar un SGSI, basado en el estándar ISO/IEC 27001:2005, en su fase de planificación.
d) Elaborar una propuesta de manual de políticas de seguridad de la información, basado en la filosofía institucional y los requerimientos del estándar ISO/IEC 27001:2005.

1.7 Metodología de la investigación

1.7.1 Definición del método de recolección de información.

El método de investigación se define de acuerdo a sus objetivos y las características de la información requerida en cada etapa de su desarrollo. De tal modo que se realizó un tipo de investigación explicativa basada en la búsqueda bibliográfica, entrevistas y observaciones de campo que permiten a partir de un diagnóstico de la situación actual, generar una propuesta de mejora.

Por tanto, en primer lugar se realizó una investigación bibliográfica en relación a la conceptualización, contexto y requerimientos del estándar ISO/IEC 27001:2005 a fin de su interpretación y aplicación en la Institución. A continuación, se realizó la investigación bibliográfica concerniente a su estructura, organización, destinatarios y operaciones comerciales.

Luego de la investigación bibliográfica, el estudio se basa principalmente en las observaciones de campo de las operaciones de la institución y la entrevista a personal clave en relación a los requerimientos del estándar. Dado que ésta no cuenta con procedimientos establecidos para sus operaciones, no es posible realizar un muestreo de procesos y en su defecto se observan aquellas consideradas relevantes; para la fase de entrevista la selección se realiza en función de la estructura organizativa y su relación con las operaciones críticas de la misma. Adicionalmente se emplea el benchmarking para capitalizar experiencias de otras instituciones que operan en El Salvador y que hayan implementado un SGSI.

1.7.2 Fuentes de investigación

a) Investigación Bibliográfica

Comprendió la consulta de textos históricos de la Institución, consulta de la información pública en su página web relacionada con proyectos, filosofía, organización y todo documento interno relacionado con la investigación. Además, la consulta de estándares de la industria, normativos, entre otros.

b) Investigación de campo

Esta investigación comprendió el diseño de seis modelos de entrevista dirigidas a personal clave en relación a la seguridad de la información y de acuerdo a su ámbito de actuación, entre este recurso clave se consideró tres niveles jerárquicos incluyendo la Dirección Ejecutiva, tres gerencias y dos coordinadores de área

involucrados. Por otro lado, se realizó la observación en sitio de las instalaciones dedicadas al procesamiento de la información y áreas críticas.

Adicionalmente se realizó un Benchmarking a dos instituciones identificadas por sus operaciones en nuestro país y la implementación de un SGSI, de tal modo de retomar sus experiencias en el diseño del SGSI para la Institución objeto de estudio.

1.8 Variables a considerar

Considerando el objetivo general y objetivos específicos, se define las macrovariables y microvariables de estudio que se muestran en la tabla 1.2.

Tabla 1.2: Macrovariables y Microvariables de estudio.

MACROVARIABLES	MICROVARIABLES
Aspectos organizativos de la seguridad de la información	Organización interna Responsabilidad relativa a la seguridad de la información. Política de seguridad de la información Responsabilidad vinculada al acceso de terceros.
Seguridad física y del entorno	Protección y seguridad de los equipos Controles físicos de entrada Mantenimiento de los equipos
Comunicaciones y operaciones	Procesos documentados Control de accesos Intercambio de información Gestión de seguridad de las redes Desarrollo y mantenimiento de sistemas de información
Gestión de incidentes en la seguridad de la información	Continuidad del negocio Acciones ante incidentes

Fuente: Elaboración propia a partir de requerimientos del estándar internacional ISO/IEC 27001:2005

CAPÍTULO II. MARCO TEÓRICO

Inmersos en una era de la información y el uso de las Tecnologías de la Información y las Comunicaciones (TIC´s) en diversos ámbitos como la educación, industria, negocios, entre otros; la información representa un bien invaluable que demanda una garantía de disponibilidad, confidencialidad e integridad; para ello las empresas deben comprometerse con estos atributos para asegurar las operaciones propias del negocio, donde la información es procesada, transmitida y almacenada.

Considerando una definición de seguridad de la información, el estándar ISO/IEC 17799 sobre el Código para la práctica de la gestión de la seguridad de la información, establece que "La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales."[5] Por otro lado, el estándar ISO/IEC 27001:2005 sobre el Sistema de Gestión de Seguridad de la Información (SGSI) define la seguridad de la información como "preservación de la confidencialidad, integridad y disponibilidad de la información; además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confidencialidad"[6]

En este contexto y retomando estas definiciones, existe una variedad de normas, estándares y buenas prácticas orientadas a la seguridad de la información, en su mayoría bajo la perspectiva técnica de la seguridad. Sin embargo, conscientes de que el tema de seguridad de la información no puede ser abordado solamente en una perspectiva técnica, que muchos de los incidentes de seguridad se asocian a

[5] Estándar Internacional ISO/IEC 17799 Código para la práctica de la gestión de la seguridad de la información.
[6] Anexo 1: Estándar Internacional ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información.

las practicas del recurso humano y que el compromiso de la organización debe ser adoptado por todos los niveles jerárquicos, se toma como referencia el estándar ISO/IEC 27001:2005 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos, ya que es un estándar que aborda de manera integral los aspectos organizativos, técnicos y operativos de la seguridad de la información bajo un enfoque de mejora continua aplicable a todo tipo de organizaciones independientemente de su tamaño, naturaleza, y giro de negocio.

2.1 Definición del estándar internacional ISO/IEC 27001:2005 Tecnología de la información – Técnicas de seguridad – Sistema de gestión de seguridad de la información – Requerimientos.

El estándar para la seguridad de la información ISO/IEC 27001:2005 (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en octubre de 2005 por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) y por la Comisión Electrotécnica Internacional (IEC, International Electrotechnical Commission), la cual especifica los requisitos necesarios para establecer, implementar, operar, monitorear y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

El Estándar comprende:

a) Introducción general
b) Enfoque de procesos
c) Compatibilidad con otros sistemas de gestión
d) Alcance: general y aplicación
e) Referencias normativas
f) Términos y definiciones

g) Sistema de gestión de seguridad de la información: requerimientos generales, establecer y manejar el SGSI, requerimientos de documentación.
h) Responsabilidad de la gerencia: Compromiso y gestión de recursos
i) Auditorías internas del SGSI
j) Revisión gerencial del SGSI

Este estándar se basa en un modelo con enfoque a procesos para la gestión de la seguridad de la información, conocido como PDCA por sus siglas en inglés (Planear, hacer, chequear, actuar), donde se enfatiza la importancia y propósito de:[7]

a) Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
b) Implementar y operar controles para manejar los riesgos de la seguridad de la información;
c) Monitorear y revisar el desempeño y la efectividad del SGSI; y
d) Mejoramiento continuo en base a la medición del objetivo.

El modelo exige que la organización establezca, implemente, opere, monitoree, mantenga y mejore continuamente un SGSI documentado en base al contexto de las operaciones comerciales generales de la organización y los riesgos a los que se está expuesto.

En la figura 2.1, se muestra el esquema del modelo como un ciclo continuo de cuatro etapas en función del SGSI, las expectativas y resultados de las partes interesadas, donde se implementa y opera, establece, mantiene, monitorea y revisa el SGSI.

[7] Anexo 1: Estándar Internacional ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información.

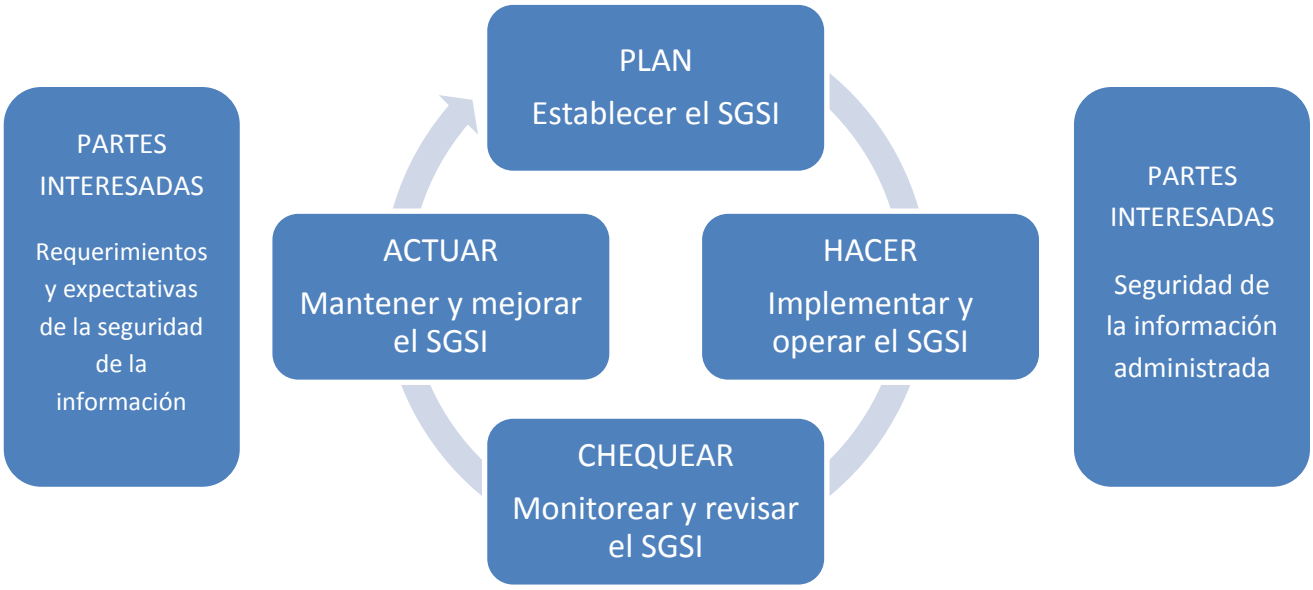


Figura 2.1: Modelo PDCA aplicado a los procesos del SGSI

El estándar es compatible con otros sistemas de gestión, tal es el caso de ISO 9001:2000 Sistema de Gestión de la Calidad e ISO 14001:2004 Sistema de Gestión Ambiental, conformando un sistema integrado cuyo alcance comprende todo tipo de organizaciones.

Por tanto, implementar un modelo de SGSI en cualquier organización tiene como objetivo:

a) Identificar los riesgos para la organización en función de la seguridad de la información.
b) Establecer los controles ante los riesgos de seguridad de acuerdo a las vulnerabilidades identificadas.
c) Definir las políticas del SGSI dentro de la organización.
d) Evaluar y medir el proceso de desempeño y eficiencia del modelo.
e) Tomar acciones ante incidentes de seguridad.
f) Implementar acciones correctivas y preventivas basadas en resultados de auditoria y seguimiento para mejorar continuamente el SGSI.

2.2 Sistema de Gestión de Seguridad de la Información

El SGSI es entonces un conjunto de políticas y procesos para gestionar, de manera eficiente, la accesibilidad a la información, asegurando su confidencialidad, integridad y disponibilidad de los activos, minimizando los riesgos de seguridad de la misma.

Por tanto, de acuerdo al estándar internacional ISO/27001:2005, la implementación del SGSI requiere que las organizaciones[8]:

a) Definan el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles y la justificación de cualquier exclusión del alcance.

b) Definan una política del SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología, que además:
    a. Incluyan un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información;
    b. Tomen en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual;
    c. Estén alineadas con el contexto de la gestión estratégica del riesgo de la organización, en el cual se establecerá y mantendrá el SGSI;
    d. Establezcan el criterio con el que se evaluará el riesgo;
    e. Hayan sido aprobadas por la gerencia.

c) Definan el enfoque de valuación del riesgo de la organización.

[8] Anexo 1: Estándar Internacional ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información

a. Identifiquen una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.
b. Desarrollen los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables.

d) Identifiquen los riesgos.
    a. Identifiquen los activos dentro del alcance del SGSI y los propietarios de estos activos.
    b. Identifiquen las amenazas para éstos activos.
    c. Identifiquen las vulnerabilidades que podrían ser explotadas por las amenazas.
    d. Identifiquen los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

e) Analicen y evalúen el riesgo.
    a. Calculen el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.
    b. Calculen la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.
    c. Calculen los niveles de riesgo.
    d. Determinen si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo.

f) Identifiquen y evalúen las opciones para el tratamiento de los riesgos
    a. Apliquen los controles apropiados;

b. Acepten los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo de la organización;
c. Eviten los riesgos; y
d. Transfieran los riesgos comerciales asociados a otras entidades.

g) Seleccionen objetivos de control y controles para el tratamiento de riesgos.
h) Obtengan la aprobación de la gerencia para los riesgos residuales propuestos.
i) Obtengan la autorización de la gerencia para implementar y operar el SGSI.
j) Prepararen un Enunciado de Aplicabilidad que incluya:
    a. Los objetivos de control y los controles seleccionados y las razones para su selección
    b. Los objetivos de control y controles implementados actualmente; y
    c. La exclusión de cualquier objetivo de control y la justificación para su exclusión.

En el anexo A del estándar, se presentan 39 objetivos de control como referencia para la selección de controles en el SGSI; estos están relacionados con 133 controles comúnmente relevantes para las organizaciones. En la tabla 2.1 se muestra un detalle del ámbito o alcance de control de seguridad considerados en el estándar; posteriormente en el Capítulo III se hace referencia a los controles por cada ámbito.

Tabla 2.1 Ámbitos de control de seguridad

OBJETIVOS DE CONTROL Y CONTROLES DEL ESTANDAR ISO27001:2005		
Apartado del estándar	**Ámbito**	**Subámbito**
5	Política de seguridad	5.1 Política de seguridad de la información.
6	Organización de la seguridad	6.1 Organización interna 6.2 Entidades externas.
7	Gestión de activos	7.1 Responsabilidad por los activos. 7.2 Clasificación de la información.
8	Seguridad de los recursos humanos	8.1 Antes del empleo. 8.2 Durante el empleo. 8.3 Terminación o cambio de empleo.

Apartado del estándar	Ámbito	Subámbito
9	Seguridad física y del entorno	9.1 Áreas seguras. 9.2 Seguridad del equipo.
10	Gestión de comunicaciones y operaciones	10.1 Procedimientos y responsabilidades operativas. 10.2 Gestión de la entrega del servicio a terceros. 10.3 Planeación y aceptación del sistema. 10.4 Protección contra software malicioso y código móvil. 10.5 Respaldo (Back-up). 10.6 Gestión de seguridad de redes. 10.7 Gestión de medios. 10.8 Intercambio de información. 10.9 Servicios de comercio electrónico. 10.10 Monitoreo.
11	Control de acceso	11.1 Requerimiento comercial para el control de acceso. 11.2 Gestión de acceso del usuario. 11.3 Responsabilidad del usuario. 11.4 Control del acceso a redes. 11.5 Control de acceso al sistema operativo. 11.6 Control de acceso a aplicaciones e información. 11.7 Computación móvil y teletrabajo.
12	Adquisición, desarrollo y mantenimiento de sistemas	12.1 Requerimientos de seguridad de los sistemas. 12.2 Procesamiento correcto en las aplicaciones. 12.3 Controles criptográficos. 12.4 Seguridad de los archivos del sistema. 12.5 Seguridad en los procesos de desarrollo y soporte. 12.6 Gestión de vulnerabilidad técnica.
13	Gestión de incidentes de seguridad	13.1 Reporte de eventos y debilidades en la seguridad de la información. 13.2 Gestión de incidentes y mejoras en la seguridad de la información.
14	Gestión de continuidad del negocio	14.1 Aspectos de la seguridad de la información y la continuidad del negocio.
15	Cumplimiento	15.1 Cumplimiento con requerimientos legales. 15.2 Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico. 15.3 Consideraciones de auditoría de los sistemas de información.

Fuente: Elaboración propia a partir de los controles definidos en el estándar ISO/IEC27001:2005

2.3 Beneficios al implementar un Sistema de Gestión de Seguridad de la información

Tomar la decisión de implementar y gestionar un SGSI es una decisión de alto nivel gerencial que implica un compromiso de la organización con los objetivos del mismo; por tal razón debe contar con todo el respaldo y disponibilidad de recursos, documentos e información relevante para su desarrollo e implementación.

Iniciar este proceso y su eficiente continuidad supone algunos beneficios directos e indirectos para la organización, entre los que se puede mencionar:

a) Conocer los riesgos de seguridad y poder gestionarlos.
b) Implementar controles que minimicen los riesgos y amenazas en seguridad de la información.
c) Lograr mayor credibilidad, confianza y fiabilidad ante clientes y destinatarios.
d) Mejorar las relaciones con clientes y aliados estratégicos.
e) Mayor nivel de compromiso de parte de colaboradores y usuarios.
f) Operaciones basadas en procesos.
g) Adopción de mejores prácticas de la industria.
h) Preservación de la información.
i) Compromiso con la mejora continua.
j) Entorno de trabajo basado en procesos y compatible con otros modelos de gestión aplicados a la industria y demás sectores productivos.
k) Desarrollo de procesos que garantizan la confidencialidad, seguridad e integridad de la información.
l) Colaboradores identificados con la filosofía de la organización.

2.4 Etapas para el desarrollo de un Sistema de Gestión de Seguridad de la Información.

En el desarrollo e implementación del SGSI se pueden identificar al menos cinco etapas, las cuales contemplan desde el análisis de requerimientos hasta su seguimiento y retroalimentación.

En la figura 2.2 se muestra una propuesta que se ajusta a las necesidades y requerimientos de cualquier organización en función del desarrollo de un modelo basado en el estándar ISO/IEC 27001:2005. En esta se identifican las siguientes etapas:

a) Fase 1: Revisión de requerimientos del estándar.

En la fase 1 deben analizarse los requerimientos del estándar en la perspectiva del diagnóstico que deberá realizarse en la organización y los requerimientos del SGSI. Básicamente consiste en identificar las etapas del estudio que ya han sido definidas en este apartado y establecimiento de la estrategia para su desarrollo.

Figura 2.2 Etapas de desarrollo de un SGSI.

b) Fase 2: Diagnóstico de la organización.

El diagnóstico de la organización comprende la aplicación de técnicas de análisis orientadas al estudio documental, observaciones y prácticas dentro de la organización; para tal propósito se define la metodología a seguir y como resultado las fortalezas y debilidades de la organización en cuanto a seguridad de la información. Esta etapa brinda las pautas para establecer las recomendaciones que deberá considerar y/o implementar la organización. Comprende además la valoración de riesgos de seguridad para la organización y se define el modelo de gestión de seguridad de la información y manual de políticas de seguridad correspondiente.

c) Fase 3: Propuesta de solución

En esta etapa y considerando los resultados de la fase de diagnóstico, se define un plan de solución e implementación, identificando cada una de las etapas que deberán desarrollarse cronológicamente y además las estrategias para su ejecución.

d) Fase 4: Implementación

La fase de implementación se realiza en base al respectivo plan de implementación, indicando los resultados de cada fase de desarrollo en sus fortalezas y aspectos de mejora, así como el plan de inversión ejecutado, esta fase es propia del proyecto en ejecución e indispensable para el análisis posteriori de las fortalezas y debilidades del proceso.

e) Fase 5: Retroalimentación y monitoreo

La retroalimentación y monitoreo es clave del proceso continuo del modelo PDCA que garantiza la mejora continua de los procesos y donde se integran las etapas del SGSI orientadas a la revisión del SGSI, procesos de auditoría y mejora continua y responsabilidades. Esta etapa permite la identificación de aspectos de mejora y ajustes al proceso.

CAPÍTULO III. DIAGNÓSTICO DE FUSALMO

3.1 Contexto y capacidad instalada de FUSALMO

La Institución desarrolla todos sus programas en sus modernas y amplias instalaciones "Polideportivos y Multigimnasio Don Bosco" ubicadas en tres de las principales zonas del país: San Miguel, Santa Ana y Soyapango, en donde semanalmente se atienden un promedio de 7,500 niños, niñas y jóvenes en los distintos programas; en la tabla 3.1 se mencionan las instalaciones y algunos de sus beneficiarios.

Tabla 3.1 Polideportivos y Multigimnasio

UBICACIÓN	INFRAESTRUCTURA	BENEFICIARIOS
SOYAPANGO	Polideportivo Plaza juvenil España Multigimnasio Don Bosco	9 escuelas públicas (incluye instituciones en Ciudad Delgado)
SAN MIGUEL	Polideportivo Centro Juvenil Don Bosco	11 escuelas publicas
SANTA ANA	Polideportivo	6 escuelas publicas

Fuente: Informe de resultados 2011, presentación proporcionada por colaboradores de la Fundación e información disponible en el sitio web oficial de la Fundación

3.1.1 Programas y proyectos

Los programas y proyectos de FUSALMO se concentran en 5 áreas de apoyo detalladas en la tabla 3.2, y en las tablas 3.3, 3.4 y 3.5 se muestran algunos resultados y beneficios de los mismos.

Tabla 3.2 Programas y proyectos dirigidos por la Fundación.

ÁREA DE APOYO	PROYECTO	DESCRIPCIÓN
Educación Complementaria	Programa Integral Juvenil Don Bosco (PIJDB)	Programa de capacitación a jóvenes de tercer ciclo en temas de tecnología, educación física-deportes, cultura de paz, entre otros. Programa de capacitación a docentes de los centros escolares en temas de psicopedagogía, salud mental, entre otros.

ÁREA DE APOYO	PROYECTO	DESCRIPCIÓN
Educación Complementaria	Centro de Atención Integral a la Familia (CAIF)	Programa de atención en la relación familiar y la comunidad mediante orientación espiritual, psicológica, apoyo comunitario, entre otros.
	Tecnología e Innovación	Programa de formación en el uso y aplicación de TIC´s, enseñanza del idioma Inglés y valores humanos.
Gestión socio-laboral	Intermediación laboral	Orientación en el proceso de integración laboral y búsqueda de oportunidades.
	Emprendedurismo social	Programa de formación de jóvenes en diseño de proyectos comunitarios y promoción de valores.
	Emprendedurismo juvenil económico	Formación de jóvenes emprendedores en la elaboración de plan de negocios y su desarrollo.
	Jóvenes creando futuro	Proyectos específicos de capacitación (diseño web, mantenimiento de computadoras, diseño gráfico, entre otros)
Proyectos Especiales	Prevención de la Violencia desde el Sector Educación (PREVISE)	Orientación para la prevención y disminución de la violencia en centros escolares mediante el manejo de conflictos, capacidad de mediación, entre otros.
	Fortalecimiento de las organizaciones y expresiones juveniles locales para la convivencia en el Municipio de San Salvador	Formación en liderazgo juvenil y reconocimiento de organizaciones juveniles para su formación y participación comunitaria.
Recreación	Escuela de artes	Formación en actividades artísticas y organización de festivales y talleres.
	Escuelas deportivas	Formación técnico deportiva y educación en valores, así como desarrollo de prácticas deportivas orientadas a la sana convivencia.
Pastoral	Polioratorio FUSALMO	Programa educativo-pastoral, catequesis sacramental y relaciones interpersonales.
	Red de juventud	Espacio de análisis, discusión y aprendizaje para el fortalecimiento de valores y actitudes de liderazgo personal.

Fuente: Informe de resultados 2011, presentación proporcionada por colaboradores de la Fundación e información disponible en el sitio web oficial de la Fundación

Tabla 3.3 Resumen de atención a beneficiarios de FUSALMO año 2011

PROGRAMA	COMPONENTE	BENEFICIARIO	COSTO AL BENEFICIARIO	APOYO FINANCIERO
Programa Integral Juvenil DON BOSCO. (PIJDB)	Computación Cultura de Paz Deportes	4,500 Alumnos (30 escuelas publicas)	Sin costo	Programa institucional de gestión propia
ATENCION A LA FAMILIA Y JOVENES CON PROBLEMAS DE APRENDIZAJE	Apoyo psicopedagógico Psicológico Escuela para padres -Proyectos comunitarios		Sin costo	CESAL-Andalucía
HABILITANDO OPORTUNIDADES PARA LA PAZ Y EL EMPLEO (HOPE)	Computación Ingles, Cultura de paz, Orientación vocacional y profesional Apoyo en busca de empleo	400 alumnos de bachillerato	Sin costo	Fundacion PESTALOZZI SUIZA
APOYO AL PIJDB	Arte, cultura y empleo	4,500 Alumnos (30 escuelas publicas)	Sin costo	CESAL -AECID

Fuente: Informe de resultados 2011, presentación proporcionada por colaboradores de la Fundación e información disponible en el sitio web oficial de la Fundación

Tabla 3.4 Reporte de estadísticas de atención a beneficiarios de FUSALMO año 2011

PROGRAMA	COMPONENTE	No. DE BENEFICIARIOS	MUJERES	HOMBRES	EDADES
ESCUELAS DEPORTIVAS	AEROBICOS	68	67	1	Desde 27 a 62 años
	ATLETISMO	30	16	14	Desde 8 a 45 años
	FUTBOL	35	0	35	Desde 7 a 12 años
	TAEKWONDO	64	6	58	Desde 8 a 23 años
	PATINAJE	30	27	3	Desde 7 a 16 años
Transferencia tecnológica para empleabilidad de jóvenes en riesgo	Deporte, arte y recreación	80	12	68	18 a 25 años
MULTIGIMNASIO Educación en tiempo libre	Escuela de Música	28	21	7	6-43
	Tae Kwon Do	44	9	35	6-25
	Badminton	10	6	4	8-21
	Gimnasio Pesas	160	40	120	16-47
	Cardiovascular	24	22	2	18-40
Emprendedores Sociales	Emprendedores sociales	43	17	26	14-23
Programa de CESAL	Aula Animada	79	22	57	
	Escuela de Padres y Madres	1.150	900	250	
PIJDB Soyapango	Bachillerato	240	97	143	16 - 20 años
	6º.7º,8º, 9°	2562	1276	1286	12-17 años de edad

Fuente: Informe de resultados 2011, presentación proporcionada por colaboradores de la Fundación e información disponible en el sitio web oficial de la Fundación

Tabla 3.5 Reporte de estadísticas de atención a beneficiarios FUSALMO año 2009

PROGRAMA	COMPONENTE	No. DE BENEFICIARIOS	MUJERES	HOMBRES	EDADES
HOPE Habilitando Oportunidades Para la Paz y el Empleo juvenil	Empleabilidad, HOPE en Soyapango	38	11	27	16-19 años
BUSCANDO UN CAMINO	Reinserción	13	0	13	12 a 17 años
	Patio de día	4	0	4	15 y 16 años
	Abordaje/acogida	8	0	8	14 a 16 años
ORATORIA	TORNEO FUTSALA	783	81	702	12 a 62 AÑOS
	SACRAMENTAL	120	70	50	10 a 15 AÑOS
	TORNEO BALONCESTO	120		120	18 AÑOS Y MAS
	SCOUTS	43	18	25	7 a 18 AÑOS
DEPORTES EXTREMOS	BREAKDANCE	15		15	14 a 24 AÑOS
	SKATEBOARDING	41	6	35	7 a 31 AÑO
	BICI EXTREMO	18		18	18 AÑOS Y MAS
	DANZA MODERNA	37		37	18 a 20 AÑOS
	DANZA PIJDB	48	30	18	12 a 16 AÑOS
TOTALES		**7974**	**3776**	**4198**	

Fuente: Informe de resultados 2011, presentación proporcionada por colaboradores de la Fundación e información disponible en el sitio web oficial de la Fundación

Es así como la Institución tiene impacto en una cantidad significativa de familias y jóvenes que requieren del desarrollo de proyectos integrales para lograr una calidad de vida superior. Para lograr el esfuerzo conjunto cuenta con socios y aliados comerciales, que mediante su labor social canalizan parte de sus fondos para que FUSALMO pueda cubrir las necesidades de los proyectos y programas en marcha. Entre ellos se puede mencionar:

a) Fundación TCS
b) TIGO El Salvador
c) Microsoft
d) Embajada de los Estados Unidos de América
e) DISZASA S.A de C.V.
f) Banco HSBC
g) Almacenes Siman
h) United States Agency International Development (USAID)
i) Fundación Gloria Kriete
j) Productos Alimenticios DIANA
k) OXGASA S.A. de C.V.
l) Agencia Española de Cooperación Internacional para el Desarrollo
m) Entre otros.

De modo que, el desarrollo de una propuesta y posterior implementación de un sistema de gestión de seguridad de la información, basado en el estándar ISO/IEC 27001:2005, vendrá a generar más seguridad en los socios y aliados de la Fundación y mejorar la gestión y administración de la información. Por lo que con este fin, se realizó la investigación con el apoyo directo de la Gerencia de Tecnología e Innovación, dependencia inmediata de la Dirección Ejecutiva, cuya estructura organizativa se presenta en la figura 3.1.

Organigrama de la Gerencia de Tecnología e Innovación

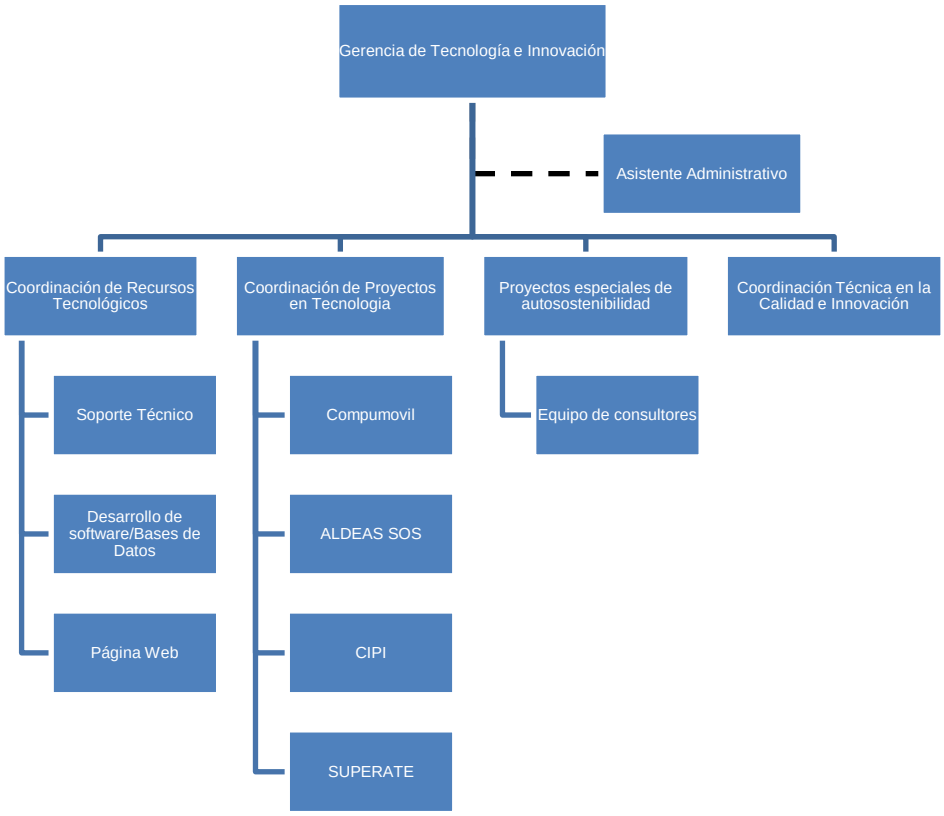


Figura 3.1 Organigrama de la Gerencia de Tecnología e Innovación de FUSALMO

En la figura 3.1 se observan tres niveles jerárquicos organizados en cuatro áreas: Coordinación de proyectos en tecnología, Proyectos especiales de autosostenibilidad, Coordinación técnica en calidad e innovación y Coordinación de recursos tecnológicos; siendo esta última la principal involucrada en el proceso.

3.2 Descripción de la metodología de diagnóstico.

En el proceso de definición del SGSI y habiendo establecido como referente el estándar ISO/IEC 27001:2005 y sus requerimientos; es indispensable la realización de un diagnóstico para la Institución en relación a la seguridad de la información. Es oportuno señalar que no se han encontrado referencias de una

metodología concreta a desarrollar para este tipo de estudio, por lo que a continuación se presenta una metodología cuyos resultados permiten identificar las necesidades de la Institución enfocado a los procesos críticos que ésta desarrolla.

Para este propósito se relacionó dos componentes: uno de ellos es los requerimientos del estándar internacional y el segundo el contexto actual de la Institución, aplicando técnicas orientadas al análisis documental, observaciones y prácticas dentro de la misma.

El diagnóstico se realiza en base a 39 objetivos y 133 controles definidos en el estándar, organizados en 11 ámbitos o categorías; cada objetivo describe el propósito, y los controles que le corresponden especifican las condiciones de realización. Estos controles se orientan no sólo a la administración de la seguridad de la información, sino además a su planificación, operativización y retroalimentación. En la tabla 3.6 se muestran los ámbitos y subámbitos relacionados con los controles requeridos en el estándar, los cuales representan a las variables de análisis.

Tabla 3.6 Ámbitos de control de seguridad y controles de seguridad.

Apartado del estándar	Ámbito	Subámbito	Objetivos de control	Controles
5	Política de seguridad	5.1 Política de seguridad de la información.	1	2
6	Organización de la seguridad	6.1 Organización interna 6.2 Entidades externas.	2	11
7	Gestión de activos	7.1 Responsabilidad por los activos. 7.2 Clasificación de la información.	2	5
8	Seguridad de los recursos humanos	8.1 Antes del empleo. 8.2 Durante el empleo. 8.3 Terminación o cambio de empleo.	3	9

Apartado del estándar	Ámbito	Subámbito	Objetivos de control	Controles
9	Seguridad física y del entorno	9.1 Áreas seguras. 9.2 Seguridad del equipo.	2	13
10	Gestión de comunicaciones y operaciones	10.1 Procedimientos y responsabilidades operativas. 10.2 Gestión de la entrega del servicio a terceros. 10.3 Planeación y aceptación del sistema. 10.4 Protección contra software malicioso y código móvil. 10.5 Respaldo (Back-up). 10.6 Gestión de seguridad de redes. 10.7 Gestión de medios. 10.8 Intercambio de información. 10.9 Servicios de comercio electrónico. 10.10 Monitoreo.	10	32
11	Control de acceso	11.1 Requerimiento comercial para el control de acceso. 11.2 Gestión de acceso del usuario. 11.3 Responsabilidad del usuario. 11.4 Control del acceso a redes. 11.5 Control de acceso al sistema operativo. 11.6 Control de acceso a aplicaciones e información. 11.7 Computación móvil y teletrabajo.	7	25
12	Adquisición, desarrollo y mantenimiento de sistemas	12.1 Requerimientos de seguridad de los sistemas. 12.2 Procesamiento correcto en las aplicaciones. 12.3 Controles criptográficos. 12.4 Seguridad de los archivos del sistema. 12.5 Seguridad en los procesos de desarrollo y soporte. 12.6 Gestión de vulnerabilidad.	6	16
13	Gestión de incidentes de seguridad	13.1 Reporte de eventos y debilidades en la seguridad de la información. 13.2 Gestión de incidentes y mejoras en la seguridad.	2	5

Apartado del estándar	Ámbito	Subámbito	Objetivos de control	Controles
14	Gestión de continuidad del negocio	14.1 Aspectos de la seguridad de la información y la continuidad del negocio.	1	5
15	Cumplimiento	15.1 Cumplimiento con requerimientos legales. 15.2 Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico. 15.3 Consideraciones de auditoría de los sistemas de información.	3	10
TOTAL			39	133

Fuente: Elaboración propia a partir de los controles definidos en el estándar ISO/IEC27001:2005

Entre las técnicas cualitativas y cuantitativas, basadas en los requerimientos del estándar, que fueron aplicadas en el estudio están:

a) Entrevista a personal clave y observación en sitio
b) Herramienta de valoración de acuerdo a los controles y requerimientos definidos en el estándar.
c) Análisis gráfico mediante la herramienta de ”Tela de araña” o análisis radial.
d) Benchmarking a empresas que operan en nuestro país y han implementado un SGSI, a fin de retomar sus experiencias en la propuesta del SGSI.
e) Además, un análisis de riesgos informáticos como requerimiento en la aplicación del estándar internacional, que también forma parte de dicho sistema.

3.2.1 Entrevista a personal clave y observación en sitio.

La técnica de entrevista a personal clave, siendo una herramienta cualitativa se diseña en base a los requerimientos de controles del estándar de referencia, considerando además el ámbito de actuación del recurso humano a entrevistar dentro de la organización y su función de seguridad de la información.

Para este propósito se diseñaron seis modelos de entrevista dirigidas a personal clave de la organización, entre los que se puede mencionar:

a) Dirección Ejecutiva
b) Gerencia de Finanzas y Recaudación de Fondos
c) Gerencia de Tecnología e Innovación
d) Gerencia de Recursos Humanos
e) Coordinación de Recursos Tecnológicos
f) Coordinación de Mantenimiento

Como característica de los modelos de entrevista se destaca además la consulta cruzada entre niveles jerárquicos relacionados, acción intencionada como medida de verificación o cruce de información proporcionada por el recurso humano. De este modo, cada colaborador entrevistado y desde su perspectiva, brindó información acerca de las condiciones de operación en la Institución en relación a la seguridad de la información.

Adicional a la entrevista, se realizó inspecciones en sitio para verificar áreas críticas como el área de servidores y área de finanzas. Además la consulta y análisis de documentación institucional para evidenciar lo declarado en las entrevistas, tal es el caso de: modelo de entrevista para empleo, contrato individual de trabajo, reglamento interno de trabajo, inventario de activos tecnológicos, bitácora de servicios técnicos, entre otros.

Para propósitos de presentación de resultados y no redundancia de información, el modelo de entrevistas se muestra en el Anexo 2 y los resultados de las mismas en la Tabla 3.22 de resumen de resultados por cada herramienta de análisis.

3.2.2 Herramienta de valoración de acuerdo a los controles y requerimientos definidos en el estándar.

En respuesta a la necesidad de cuantificar los resultados de la consulta y grado de cumplimiento con el estándar, se diseñó una herramienta de valoración, la cual integra los requerimientos de controles y objetivos establecidos en el mismo, además observaciones o comentarios que brindan una explicación de las condiciones de operación y finalmente dos tipos de valoración: una valoración estándar y una valoración a las condiciones encontradas en la Institución.

Para propósitos de análisis en esta investigación, ambas valoraciones están sujetas a una escala comprendida entre 0 (cero) a 5 (cinco); donde cero representa la ausencia o nulo cumplimiento de las condiciones para determinado control definido en el estándar y 5 representa la máxima ponderación referida a su total cumplimiento. Dentro de dicha escala se definen tres niveles de puntuación, donde 0 (cero) como ya se mencionó, representa el no cumplimiento del requerimiento, un valor entre 1 a 3 representa alguna estrategia implementada pero no documentada y valoraciones entre 4 ó 5 representan una estrategia implementada en grado aceptable y documentada.

De este modo, la valoración estándar está referida al total cumplimiento del requerimiento y la valoración a la Institución en estudio, se define de acuerdo a las condiciones encontradas mediante la entrevista, consulta documental y observación en sitio. Estos puntajes asignados a las condiciones en la Institución son promediados por criterio o subámbito y presentados en la tabla 3.7.

Tabla 3.7 Resultados por ámbito obtenidos mediante la herramienta de valoración

Dominio	Control	Objetivo	Valoración Estándar	Valoración FUSALMO	Observación
5. POLÍTICA DE SEGURIDAD					
5.1	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Proporcionar dirección gerencial y apoyo a la seguridad de la información en coherencia con los requerimientos comerciales, leyes y regulaciones.	5	0	No se tiene una política de seguridad documentada, divulgada o en proceso de revisión.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
6.1	ORGANIZACIÓN INTERNA	Administrar la seguridad de la información dentro de la organización.	5	0	Existe una organización, pero no está establecida la responsabilidad en la seguridad de la información.
6.2	ENTIDADES EXTERNAS	Mantener la seguridad de la información y los medios de procesamiento de la organización a los cuales entidades externas tienen acceso.	5	1	No se han identificado los riesgos. Hay evidencia de medidas de seguridad restrictivas en el acceso, pero no están formalmente documentadas.
7. GESTIÓN DE ACTIVOS					
7.1	RESPONSABILIDAD POR LOS ACTIVOS	Lograr y mantener la protección apropiada de los activos de la organización.	5	4	Existe un inventario de los equipos y una asignación de los mismos desde la contratación. No existe un reglamente de uso de los activos.
7.2	CLASIFICACIÓN DE LA INFORMACIÓN	Asegurar que la información reciba un nivel de protección apropiado.	5	2	Está definida las áreas críticas pero no existe un sistema de etiquetado y manejo de información.
8. SEGURIDAD DEL RECURSO HUMANO					
8.1	ANTES DEL EMPLEO	Asegurar que los empleados, contratistas y terceros conozcan sus responsabilidades y sean idóneos para los roles para los cuales se les considera y reducir el riesgo de robo, fraude o mal uso de los medios.	5	2	No se define responsabilidad sobre la seguridad en esta etapa, sin embargo se realiza investigación del perfil de los candidatos. La confidencialidad se contempla únicamente como cláusula de contrato de trabajo.
8.2	DURANTE EL EMPLEO	Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas, sus responsabilidades y obligaciones, preparados para apoyar la política de seguridad en su trabajo normal y reducir los riesgos del error humano.	5	0	No existe una política de seguridad, ni acuerdos de confidencialidad entre las partes. No se han establecido procedimientos disciplinarios en casos de violación de la seguridad de la información, ni capacitación en éste ámbito.
8.3	FINALIZACIÓN O CAMBIO DE EMPLEO	Asegurar que los empleados, contratistas y terceros salgan de la organización o cambien de empleo de manera ordenada.	5	4	Se ha implementado medidas de seguridad en la finalización del empleo, hay evidencias de devolución de activos mediante finiquito, pero estos no están documentados en un manual de procedimientos.

Dominio	Control	Objetivo	Valoración Estándar	Valoración FUSALMO	Observación
9. SEGURIDAD FISICA Y DEL ENTORNO					
9.1	AREAS SEGURAS	Evitar el acceso físico no autorizado, daño o interferencia al local y la información de la organización.	5	2	Se identificaron debilidades en el perímetro físico de las áreas de procesamiento de información, especialmente en las áreas educativas. El área de servidores está debidamente protegida en cuanto a acceso, mas no ante desastres naturales. Cuentan con sistema contra incendios en algunas áreas clave.
9.2	SEGURIDAD DEL EQUIPO	Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.	5	3	Las instalaciones no cumplen con todas las medidas de seguridad requeridas en caso de desastres. Los equipos reciben mantenimiento en caso de falla. Se tiene controles sobre el uso de los equipos fuera de las instalaciones y en su disposición final.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES					
10.1	RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN	Asegurar la operación correcta y segura de los medios de procesamiento de la información.	5	2	No se dispone de procedimientos documentados, sin embargo se tiene bitácora para el control y registro de cambios en los sistemas. Las pruebas de nuevos sistemas se realizan de manera aislada y en periodos específicos de prueba.
10.2	GESTION DE LA ENTREGA DEL SERVICIO DE TERCEROS	Implementar y mantener el nivel de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.	5	0	No se tienen controles o auditorias sobre los servicios brindados por terceros.
10.3	PLANEACION Y ACEPTACION DEL SISTEMA	Minimizar el riesgo de fallas en los sistemas.	5	4	Se monitorea la capacidad de los sistemas y se realizan diferentes niveles de prueba de los nuevos sistemas previo a su implementación.
10.4	PROTECCION CONTRA CODIGOS MALICIOSO Y MOVIL.	Proteger la información del software y código móvil.	5	5	Se dispone de un firewall y el código móvil debe ser autorizado.
10.5	COPIA DE RESPALDO	Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.	5	4	Se realizan procedimientos de Back up semanales de información de las áreas críticas. Sin embargo no está documentada una política de respaldo.
10.6	GESTION DE SEGURIDAD DE REDES	Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.	5	2	Este servicio no está garantizado ante fallas externas y no ha sido calificado por la Fundación.

Dominio	Control	Objetivo	Valoración Estándar	Valoración FUSALMO	Observación
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES					
10.7	GESTION DE MEDIOS	Evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos y la interrupción de las actividades comerciales.	5	1	No se tiene una política ni medidas de seguridad en relación al uso de medios extraíbles o manipulación e intercambio de información. La información de Back Up es custodiada.
10.8	INTERCAMBIO DE INFORMACION	Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.	5	2	Se ha implementado medidas de seguridad para el intercambio interno de la información. No se tienen políticas o procedimientos orientados al intercambio externo.
10.9	SERVICIOS DE COMERCIO ELECTRONICO	Garantizar la seguridad de los servicios de comercio electrónico y su uso adecuado.	5	1	No se realizan operaciones comerciales en línea debido a que la infraestructura actual no permite garantizar la seguridad de la información.
10.10	MONITOREO	Detectar actividades de procesamiento de la información no autorizadas.	5	1	No se realizan auditorías informáticas y no se tiene procedimientos de monitoreo establecidos. No obstante se monitorea las operaciones en redes y áreas críticas como contabilidad. Se lleva registro en bitácora acerca de las operaciones de los sistemas.
11. CONTROL DE ACCESO					
11.1	REQUERIMIENTO COMERCIAL PARA EL CONTROL DEL ACCESO	Controlar el acceso a la información	5	0	No existe una política de control de acceso documentada.
11.2	GESTIÓN DEL ACCESO DEL USUARIO	Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.	5	3	Existe un procedimiento no documentado para la inscripción y suspensión de acceso a los sistemas de información; la asignación de privilegios se realiza mediante un proceso formal.
11.3	RESPONSABILIDADES DEL USUARIO	Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.	5	2	Se brinda recomendaciones al usuario para el buen uso del equipo y la seguridad de las sesiones y contraseñas, incluso cuando los equipos están solos, pero éstas no están documentadas ni divulgadas entre todos los usuarios.
11.4	CONTROL DE ACCESO A REDES	Evitar el acceso no autorizado a los servicios en red	5	4	Los usuarios tienen restricciones de acceso por configuración de firewall y sólo pueden conectarse a los sistemas desde los equipos autorizados.

Dominio	Control	Objetivo	Valoración Estándar	Valoración FUSALMO	Observación
11. CONTROL DE ACCESO					
11.5	CONTROL DE ACCESO AL SISTEMA OPERATIVO	Evitar el acceso no autorizado a los sistemas operativos	5	4	Los accesos a los sistemas están controlados por contraseña mediante técnica autenticada de usuario y restricciones de acceso. En áreas críticas se implementa cierre de sesión por inactividad.
11.6	CONTROL DE ACCESO A APLICACIONES E INFORMACIÓN	Evitar el acceso no autorizado a la información contenida en los sistemas de aplicación	5	1	No existe una política de control de acceso, sin embargo se implementan medidas restrictivas de acuerdo a las funciones del usuario.
11.7	COMPUTACIÓN MÓVIL Y TELE-TRABAJO	Garantizar la seguridad de la información cuando se utilice medios de computación móvil y tele-trabajo	5	1	No existe una política para medios móviles, sin embargo todo dispositivo que se conecte a la red debe ser autorizado y controlado para su funcionamiento.
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN					
12.1	REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	Garantizar que la seguridad sea una parte integral de los sistemas de información	5	0	No están identificados los requerimientos de seguridad para los sistemas existentes y los nuevos.
12.2	PROCESAMIENTO CORRECTO EN LAS APLICACIONES	Evitar errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.	5	0	No se han implementado mecanismos de validación de los datos de procesamiento de información.
12.3	CONTROLES CRIPTOGRÁFICOS	Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos	5	3	No se ha establecido una política como tal, pero se implementa controles criptográficos para proteger la información.
12.4	SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA	Garantizar la seguridad de los archivos del sistema	5	3	Se han implementado medidas para restringir los derechos de usuario para instalar software no autorizado. Los datos de respaldo se realizan para las áreas críticas y estos son resguardados.
12.5	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE	Mantener la seguridad del software e información del sistema de aplicación	5	3	Se han implementado algunas medidas de seguridad en los procesos de desarrollo y prueba de sistemas; todas las modificaciones requieren autorización.
12.6	GESTIÓN DE LA VULNERABILIDAD TÉCNICA	Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas	5	2	La información relativa a los aspectos técnicos se registra en bitácora, pero ésta no es utilizada como fuente para identificación de vulnerabilidades.

Dominio	Control	Objetivo	Valoración Estándar	Valoración FUSALMO	Observación
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN					
13.1	REPORTE DE EVENTOS Y DEBILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN	Asegurar que la información acerca de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información, sea comunicada de manera que permita tomar una acción correctiva oportuna.	5	2	No existe un procedimiento formal para reportar incidentes de seguridad de la información, ni una cultura de monitoreo por parte de todos los usuarios.
13.2	GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.	5	1	No existe una gestión de incidentes como tal; sin embargo su ocurrencia ha forzado la conciencia y la implementación de medidas preventivas ante estos. Los riesgos no son cuantificados.
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO					
14.1	SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE CONTINUIDAD DEL NEGOCIO	Contrarrestar las interrupciones de las actividades y proteger los procesos comerciales críticos de los efectos de las fallas o desastres importantes en los sistemas de información y asegurar su reanudación oportuna.	5	1	Se han identificado las áreas críticas del negocio pero no se tienen planes de continuidad del mismo.
15. CUMPLIMIENTO					
15.1	CUMPLIMIENTO DE REQUERIMIENTOS LEGALES	Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.	5	3	Se rinde cuentas a través de procesos de auditoría externa ante los organismos reguladores de licencias y derechos de autor. No existe una adopción de regulaciones específicas.
15.2	CUMPLIMIENTO CON LAS POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y REQUERIMIENTOS TÉCNICOS	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.	5	3	A pesar no haber una regulación, la administración es responsable en la implementación y monitoreo de los sistemas de información acorde a los lineamientos institucionales.
15.3	CONSIDERACIONES DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN	Maximizar la efectividad y minimizar la interferencia del proceso de auditoría de los sistemas de información.	5	0	No se realiza auditoria informática

Fuente: Elaboración propia a partir de investigación realizada en FUSALMO aplicando herramienta de valoración cuantitativa y los requerimientos del estándar ISO/IEC 27001:2005.

3.2.3 Análisis gráfico mediante herramienta de ”Tela de araña” o gráfico radial.

El análisis gráfico mediante la tela de araña o análisis radial, se fundamenta en los resultados cuantitativos de la herramienta de valoración descrita en el apartado 3.2.2, permitiendo visualizar los ámbitos más débiles, así como las fortalezas en relación a los requerimientos del estándar de referencia.

Por tanto, en las figuras 3.2, 3.3 y 3.4 se muestran las brechas entre el requerimiento del estándar y lo observado, las cuales están representadas por los puntos más cercanos al centro del gráfico. De modo que, se destaca la necesidad de iniciar acciones de fortalecimiento con el propósito de eliminar estas brechas hacia un proceso de implementación del modelo de seguridad de la información.

En la figura 3.2 se identifican algunas áreas críticas con indicadores bajos:

a) Políticas
b) Organización de la seguridad
c) Procesos internos con usuarios
d) Gestión de la entrega del servicios de terceros

Los demás ámbitos representados muestran algún grado de avance de gestión y en su mayoría son correspondientes con la ejecución de procesos.

En la figura 3.3, se observa la valoración de los aspectos técnicos y operativos de la seguridad de la información, donde se destacan tres necesidades:

a) la definición de los requerimientos para el control de acceso para los usuarios,
b) el control de acceso a las aplicaciones e información;
c) y monitoreo.

Los literales a) y b) están vinculados directamente a la identificación de riesgos y las políticas que deberán implementarse en el corto y mediano plazo. En conjunto los tres elementos se visualizan desde una perspectiva de definición de una política de seguridad y los controles necesarios para la operativización y garantía de seguridad en las operaciones.

Figura 3.2: Resultados de valoración de los ámbitos 5, 6, 7, 8, 9 y 10

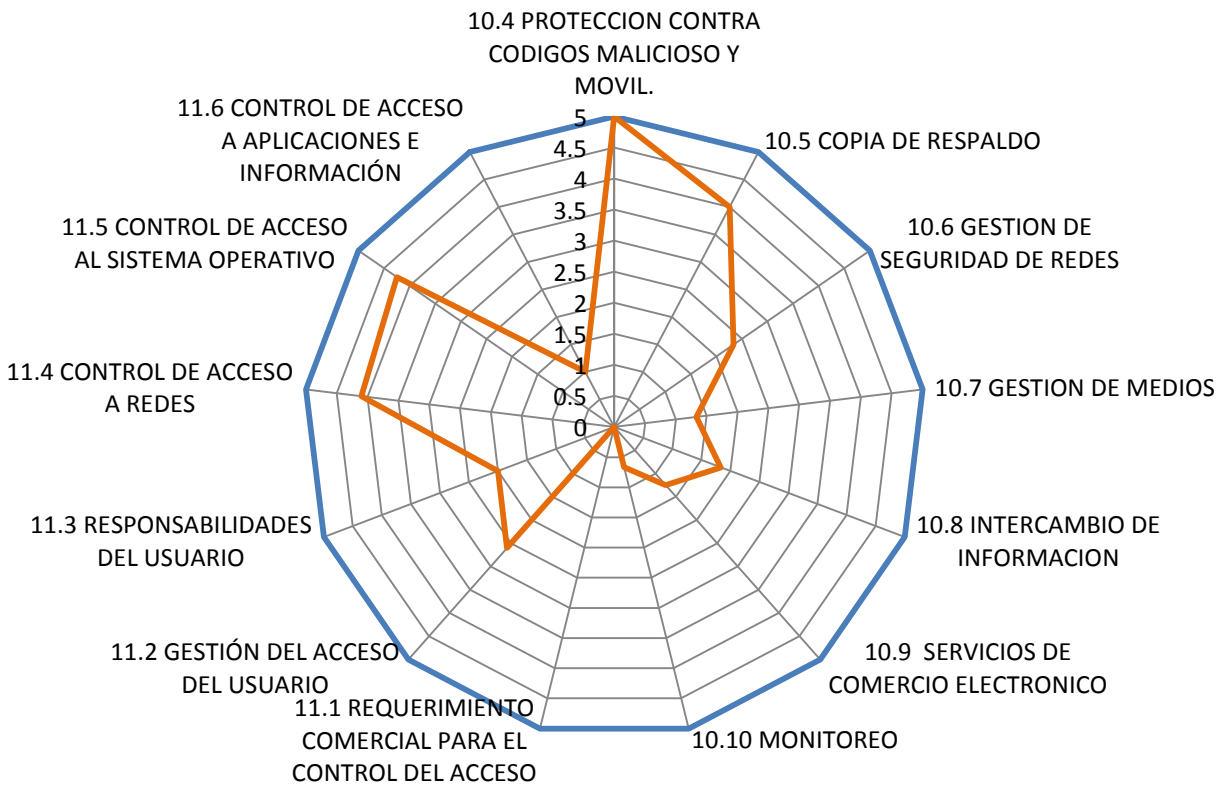


Figura 3.3: Resultados de valoración de los ámbitos 10 y 11

En la figura 3.4, se identifica nuevamente tres factores críticos de mejora relacionados con los incidentes de seguridad;

a) Auditoría de los sistemas de información.
b) Gestión de incidentes y mejoras en la seguridad.
c) Requerimientos de seguridad y monitoreo de los sistemas y aplicaciones.

RESULTADOS DE VALORACIÓN POR CRITERIOS DEL ESTANDAR ISO/IEC27001:2005
AMBITOS 11 ,12, 13, 14 Y 15
DIAGNÓSTICO FUSALMO 2012

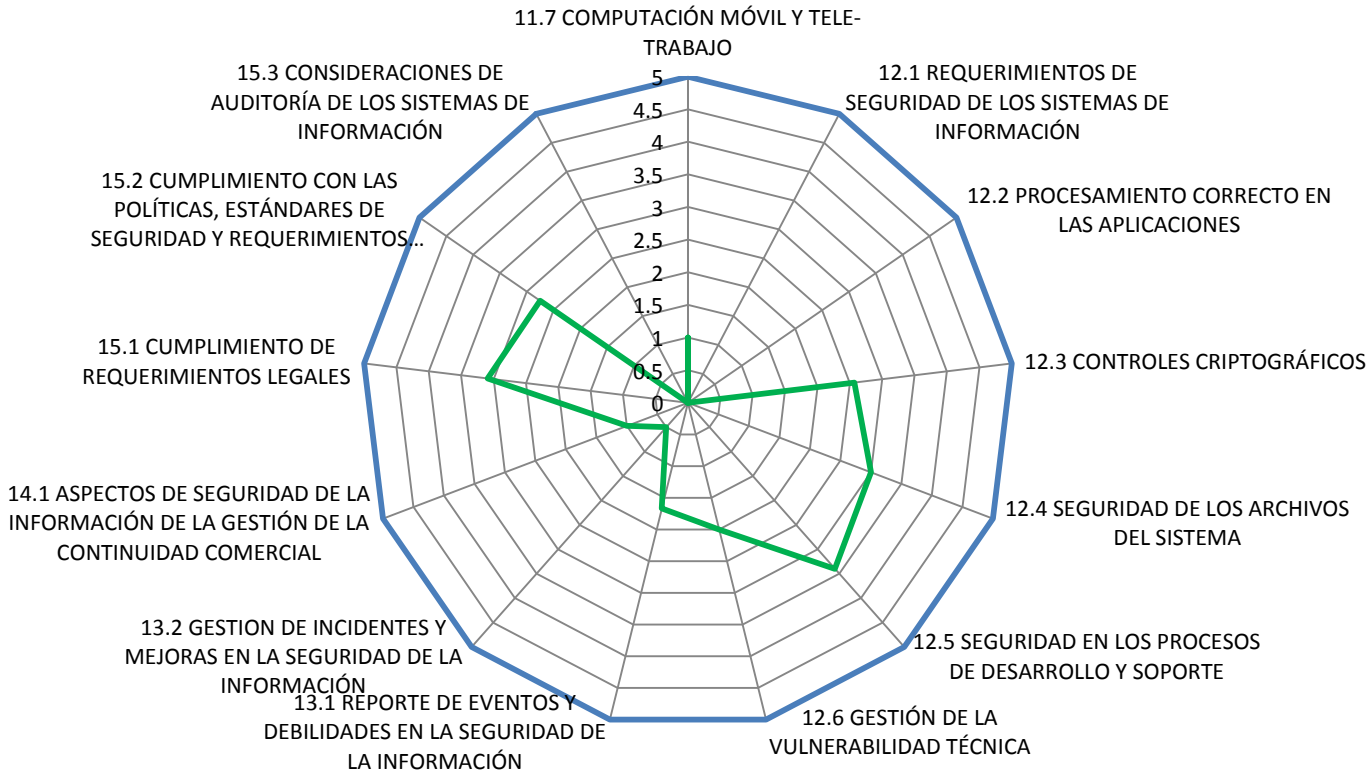


Figura 3.4: Resultados de valoración de los ámbitos 11, 12, 13, 14 y 15

3.3 Análisis de riesgos

La implementación de un SGSI demanda el establecimiento de una metodología de análisis de riesgos que permita identificar las vulnerabilidades y amenazas que deberán considerarse en el seguimiento y mejora del mismo. Por lo que en esta investigación el análisis se realizó mediante la herramienta OCTAVE

(Operationally Critical Threat, Asset, and Vulnerability Evaluation) que se describe a continuación.[9]

3.3.1 Metodología OCTAVE

El método OCTAVE es una estrategia de valoración subjetiva basada en riesgos y técnicas de planificación de la seguridad; desarrollado por el Coordination Center (CERT) del Instituto de Ingeniería de Software (Software Engineering Institute) de la Universidad Carnegie Mellon de Pensilvania, Estados Unidos.

Básicamente aplica un enfoque de tres fases para análisis de riesgos en tres perspectivas: organización, tecnología y prácticas enfocadas a la seguridad. Es por esta razón que presenta idoneidad para su aplicación en este análisis, ya que integra una visión global de las necesidades de seguridad de la información.

Las tres fases que componen el método son:

a) Identificar los elementos críticos y las amenazas a los activos.
b) Identificación de las vulnerabilidades, tanto organizativas y tecnológicas, que se exponen a las amenazas y ponen en riesgo a la organización.
c) Desarrollo de una estrategia de protección basada en la práctica y los planes de mitigación de riesgos para apoyar la misión de la organización.

En esta metodología, los activos incluyen personas, hardware y software, información y sistemas; los cuales se seleccionan según la importancia que representan para los objetivos de la organización, las posibles amenazas y vulnerabilidades asociadas a estos y el impacto de un problema asociado al activo.

[9] http://www.cert.org/octave/octavemethod.html

La metodología parte de un proceso consultivo al personal involucrado para explotar el conocimiento de los múltiples niveles de la organización, sus prácticas y recursos tecnológicos, permitiendo:

a) Identificar los activos críticos
b) Identificar las amenazas para estos activos
c) Identificar vulnerabilidades
d) Identificar el impacto que puedan tener las pérdidas de confidencialidad, integridad y disponibilidad de los activos.
e) La probabilidad de ocurrencia de una falla
f) Y los niveles de riesgo.

De modo que, la identificación de los riesgos a los activos más críticos se emplea para priorizar áreas de mejoramiento y estrategias de seguridad para la organización. Por tanto, a continuación se desarrollan estas etapas, retomando para ello el proceso consultivo antes descrito en este capítulo.

3.3.1.1 Identificación de los activos críticos de la Institución

A partir del inventario de activos de FUSALMO, en la tabla 3.8 se muestran los activos de información de la Fundación, clasificados en cuatro categorías.

Tabla 3.8 Descripción de activos de información de FUSALMO

Categoría	Activos
SISTEMAS	a) Correo Institucional Hosting Externo (hostgator) b) Página Web Hosting Externo. c) Sistema Administrativo Financiero. (SAF) d) Sistema de Recursos Humanos. e) Office 365. (En Ejecución)
INFORMACION	a) Base de Datos Institucional. (SIIPDB) b) Sistema de Intermediación Laboral. c) Sistema de Fomento al Emprendedurismo.

Categoría	Activos
SOFTWARE	a) 300 Licencias Windows XP. b) 150 Licencias Windows 7. c) 350 Licencias de Office 2010. d) 250 Licencias de Office 2007 e) 24 Licencias Office 2011 MAC f) 20 Licencias OS X Snow Leopard (MAC) g) 4 Licencias OS X Mountain Lion (MAC) h) 4 Licencias Adobe Maste Collection i) 350 Licencias Nod32 Endpoint j) Licencia Windows Server 2003 k) Licencia Windows Server 2008 R2 l) Licencia de MindManager m) Licencia Visual Studio 2010 n) 2 Licencias Win7-MAK o) 2 Licencias Windows Vista KMS p) 2 Licencias Windows Vista MAK q) 4 Licencias Windows XP profesional r) 2 Licencias Windows XP Tablet PC Edition s) Licencia Visual Studio Professional 2008 Edition t) Licencia Entourage 2008 for MAC u) Licencia Entourage 2008 for MAC with SP2 v) Expression Web 3.0 w) 2 Licencias Office communicator 2007 x) 2 Licencias Office Multilanguage Packs 2007 y) Licencia Office Multilanguage Packs 2007 service pack 1 z) 2 Licencias Office professional Plus 2007 aa) Licencia Office professional Plus 2010 MAK bb) Licencia Office Small Business 2007 cc) Licencia Office XP applications dd) Licencia Office XP Suites ee) Licencia Project Professional 2007 ff) Licencia Project Professional 2010 MAK gg) Licencia Win srv 2008 Data ctr/Itan KMS C hh) 5 Licencias Windows server 2003 ii) 1 Licencia Windows server 2008 jj) Licencia Windows web/HPC Srv 2008 KMS kk) Licencia Windows web/HPC Srv 2008 MAK ll) 4 Licencias Office professional 2003.
HARDWARE	Infraestructura de red: a) 4 Switch 3Com 2250 sfp b) 3 Switch 3Com 2226 sfp

Categoría	Activos
	c) 1 Switch Allied Telesis d) 7 Switch 3Com 4226T e) 2 Router Cisco 2600 f) 4 Media Converter g) 2 Firewall WacthGuard 55e h) 1 Firewall WacthGuard 550e i) 4 Cisco Linksys 300n j) Servidores: k) 4 Servidores de red HP / LIEBERT 2KVA l) 20 Computadoras Notebook (PC Portátil) m) 183 Computadoras desktop, monitor, teclado, mouse, cpu. n) 33 Impresores o) 4 Scanner p) 50 UPS q) 15 Webcam r) 1 Equipo de diseño gráfico: PC, UPS, monitor y periféricos. s) 6 Monitores t) 8 CPU

Fuente: Elaboración propia a partir del inventario de activos de FUSALMO

Adicional a lo anterior, para propósitos de esta herramienta de análisis, se considera activo al personal del área de Tecnología e innovación que tiene acceso a información confidencial, así como también el personal del área contable y demás usuarios de los sistemas de aplicación. Luego a partir de la tabla 3.8 se seleccionan los activos imprescindibles en las operaciones, considerando las actividades críticas de la Institución y su dependencia con estos, de modo que se seleccionan los siguientes:

a) El Sistema Administrativo Financiero (SAF)

   Sistema para el registro contable y financiero.

   Sistema crítico donde se administra información confidencial, capaz de interrumpir las operaciones comerciales en caso de pérdida o manipulación.

b) Servicio de Internet

Servicio externo para todos los clientes y colaboradores.

Servicio crítico para los objetivos educativos y las operaciones de sistemas internos.

c) Infraestructura de red

Comprende los dispositivos que permiten el funcionamiento de la red (routers, cables, servidores, switches, etc.), transmisión y direccionamiento información. Crítico en la comunicación de información.

d) Personal del área de Tecnología e Innovación

Recurso Humano que brinda soporte al equipo y a las aplicaciones.

Luego de definir los activos críticos se definen los requerimientos de seguridad para estos activos críticos en base a tres criterios: Disponibilidad, confidencialidad e integridad, tal como se muestran en la tabla 3.9.

Tabla 3.9 Requerimientos de seguridad para los activos críticos

ACTIVO CRÍTICO	**DESCRIPCIÓN**	**REQUERIMIENTOS DE SEGURIDAD PARA LOS ACTIVOS CRITICOS**		
		DISPONIBILIDAD	**CONFIDENCIALIDAD**	**INTEGRIDAD**
Sistema Administrativo Financiero (SAF)	Sistema para el registro contable y financiero de la Fundación. Sistema crítico donde se administra información confidencial, capaz de interrumpir las operaciones comerciales en caso de pérdida o manipulación.	Eficiencia en el procesamiento de la información. Disponibilidad de la información para usuarios autorizados 24/7.	Autenticación de usuarios para acceder a la información. Sesiones de acceso con advertencia de seguridad Medidas de protección de sesión de usuario ausente.	Advertencia de seguridad en la modificación de información por usuarios autorizados.

ACTIVO CRITICO	DESCRIPCION	REQUERIMIENTOS DE SEGURIDAD PARA LOS ACTIVOS CRITICOS		
		DISPONIBILIDAD	**CONFIDENCIALIDAD**	**INTEGRIDAD**
Servicio de Internet	Servicio externo para todos los clientes y colaboradores. Servicio crítico para los objetivos educativos y las operaciones de sistemas internos.	Monitoreo permanente del servicio del proveedor. Disponibilidad para usuarios autorizados 24/7 Eficiencia en el tráfico de información.	Autenticación de clientes para el acceso a correo institucional y sesiones de usuario. Protección de datos y cuentas de usuario.	Restricción de acceso según política. Aplicativos de SAF y correo electrónico deberán viajar en forma segura, mediante un SSL(security socket layer)
Infraestructura de red	Comprende los dispositivos que permiten el funcionamiento de la red (routers, clables, servidores, switches, etc.) y transmisión y direccionamiento de información. Crítico en la comunicación de información.	Completa disponibilidad de todos los puntos de la infraestructura para la comunicación de información. Disponibilidad del 100% 24/7	Restricción de acceso a terminales o personal no autorizado. Evitar manipulación no autorizada de los equipos mediante protocolos seguros para el acceso a los sistemas de administración de estos.	Política de respaldo de configuraciones. Políticas de protección de los activos.
Personal de TI	Es el equipo humano que brinda soporte al equipo y a las aplicaciones de la institución	Personal capacitado para dar soporte de TI disponible al ser requerido	Políticas de seguridad para garantizar el manejo de la información. Aplicación de estándares de servicio	Personal autorizado para cada área informática

Fuente: Elaboración propia a partir de la metodología de análisis OCTAVE y resultados del diagnóstico en FUSALMO

3.3.1.2 Identificación de las amenazas para los activos críticos

Las amenazas se definen en función cuatro categorías:

a) Acción humana relacionada con el acceso físico
b) Acción humana relacionada con el acceso de red
c) Problemas en los sistemas
d) Otros problemas

De tal modo que a cada activo crítico se le relaciona alguno de estos tipos de amenaza, tal como se muestra en la Tabla 3.10.

Tabla 3.10 Amenazas de seguridad para los activos críticos

ACTIVO CRÍTICO	DESCRIPCIÓN	AMENAZA
Sistema Administrativo Financiero (SAF)	Sistema para el registro contable y financiero de la Fundación. Sistema crítico donde se administra información confidencial, capaz de interrumpir las operaciones comerciales en caso de pérdida o manipulación.	Acción humana relacionada con el acceso físico. Acción humana relacionada con el acceso de red. Otros problemas.
Servicio de Internet	Servicio externo para todos los clientes y colaboradores. Servicio crítico para los objetivos educativos y las operaciones de sistemas internos.	Acción humana relacionada con el acceso físico. Problemas en los sistemas. Otros problemas.
Infraestructura de red	Comprende los dispositivos que permiten el funcionamiento de la red (routers, clables, servidores, switches, etc.) y transmisión y direccionamiento de información. Crítico en la comunicación de información.	Acción humana relacionada con el acceso físico. Acción humana relacionada con el acceso de red. Otros problemas.
Personal de TI	Es el equipo humano que brinda soporte al equipo y a las aplicaciones de la institución	Acción humana relacionada con el acceso físico. Acción humana relacionada con el acceso de red. Otros problemas.

Fuente: Elaboración a partir de la metodología de análisis OCTAVE y resultados del diagnóstico en FUSALMO

3.3.1.3 Identificación de vulnerabilidades para los activos críticos.

Luego de definir las amenazas, se establecen las vulnerabilidades para cada uno de los tipos de amenaza, esto se realiza a partir del diagnóstico de la Institución, donde se identificaron las siguientes debilidades asociadas a éstos.

a) La Fundación no ha calificado al proveedor de servicios de redes en la prestación de los mismos.
b) No cuenta con procedimientos documentados acerca de las operaciones en sistemas, respaldos de información, reporte de incidentes, auditoría, entre otros.
c) No posee políticas de seguridad de la información documentadas en relación al acceso a la información, gestión de riesgos, entre otros.
d) Las condiciones del área de servidores es altamente vulnerable, ya que no cuenta con medidas de seguridad física, estructural y normas aplicables ante desastres naturales o eventos provocados en el debido aseguramiento del mobiliario y equipo instalado.
e) No se tiene un control de registro de acceso a las áreas que reguardan equipo, tal es el caso de los servidores.
f) Dos personas del área de TI tienen acceso autorizado al área de servidores, sin embargo, no se tienen planes de continuidad que garanticen su disponibilidad en caso de incidentes y la continuidad del negocio.

A partir de ésta información, en la tabla 3.11 se presentan las vulnerabilidades con sus respectivas consecuencias para valoración de impacto.

Tabla 3.11: Consecuencias de las vulnerabilidades identificadas

Vulnerabilidad	**Consecuencia**
Saturación del servicio y no disponibilidad.	a) Los servicios de correo electrónico, acceso a bases de datos y sistemas internos puede verse interrumpido. b) Suspensión de servicios por falta de redundancia cuando haya problemas en el proveedor o necesidad de intervención interna de operaciones de mantenimiento.
Fallo de equipo del proveedor del servicio.	
Un solo proveedor del servicio no calificado por la Fundación.	

Vulnerabilidad	Consecuencia
No existe procedimiento documentado de Back Up del área contable o aplicaciones.	a) Riesgo de ambigüedad en la ejecución de tareas específicas por falta de procedimientos documentos. b) Ausencia de registros de referencia en la investigación de incidentes de seguridad. c) No seguimiento de medidas preventivas en base a acuerdos de buenas prácticas.
Acceso no controlado a los equipos.	
Modificación no intencionada de la información.	a) No definición de responsabilidad en la ejecución de procedimientos y acceso a la información. b) Falta de compromiso de la alta dirección con el estricto cumplimiento de las medidas de seguridad vigentes.
Acceso a información no autorizada.	
No existe una política de acceso a la red.	
Problemas o fallas en los equipos responsables de la conectividad.	a) Suspensión de servicios y de la continuidad del negocio ante daños como consecuencia de fenómenos naturales, tal es el caso de terremotos. b) Riesgo de pérdida total ante incendios u otro tipo de siniestro. c) Riesgo de pérdida en la manipulación, operaciones o mantenimiento de hardware por fallos en el montaje de equipo.
Colapso en los equipos responsables de la conectividad como resultado de desastres naturales.	
Instalaciones físicas no seguras para los activos.	
Sabotaje a la red o servidor.	
Destrucción de la red o equipo.	
Acceso físico no controlado a servidores.	a) Personal no autorizado podría tener acceso al área de servidores.
Pérdidas materiales por manipulación de equipos en área de servidores.	
Personal no autorizado puede tener acceso a la red.	
Rotación de personal y pérdida de personal capacitado.	a) Demoras en la respuesta ante incidentes de seguridad.

Fuente: Elaboración propia a partir de diagnóstico de las condiciones de FUSALMO

3.3.1.4 Definición del riesgo.

En función de las vulnerabilidades identificadas y tomando en cuenta las consecuencias de las mismas se establecen los riesgos. Estos se clasifican en cuatro tipos:

a) Revelación de información crítica
b) Modificación de información crítica
c) Destrucción o pérdida de información
d) Interrupción del acceso a información importante, software, aplicaciones o servicios.

Tabla 3.12: Clasificación de riesgos de las vulnerabilidades identificadas

Vulnerabilidad	Riesgo
Saturación del servicio y no disponibilidad.	Interrupción del acceso
Fallo de equipo del proveedor del servicio.	Interrupción del acceso
Un solo proveedor del servicio no garantizado.	Interrupción del acceso
No existe procedimiento documentado de Back Up del área contable o aplicaciones.	Revelación de información crítica
Acceso no controlado a los equipos.	Destrucción o pérdida de información
Modificación no intencionada de la información.	Interrupción del acceso
Acceso a información no autorizada.	Revelación de información crítica
No existe una política de acceso a la red.	Interrupción del acceso Revelación de información crítica.
Problemas o fallas en los equipos responsables de la conectividad.	Interrupción del acceso
Colapso en los equipos responsables de la conectividad como resultado de desastres naturales.	Interrupción del acceso
Instalaciones físicas no seguras para los activos.	Destrucción o pérdida de información
Sabotaje a la red o servidor.	Destrucción o pérdida de información Interrupción de servicios.
Destrucción de la red o equipo.	Interrupción del acceso
Acceso físico no controlado a servidores.	Modificación de información crítica
Pérdidas materiales por manipulación de equipos en área de servidores.	Interrupción del acceso

Vulnerabilidad	Riesgo
Personal no autorizado puede tener acceso a la red.	Modificación de información crítica. Interrupción del acceso.
Rotación de personal y pérdida de personal capacitado.	Destrucción o pérdida de información. Interrupción del acceso.

Fuente: Elaboración propia a partir de diagnóstico de las condiciones de FUSALMO

3.3.1.5 Impacto de las vulnerabilidades.

Para valorar el impacto de las vulnerabilidades, se estableció la escala bajo, medio y alto, así como los umbrales de la misma para cada uno de los activos críticos, los cuales se presentan en la tabla 3.13. Con esta escala se valoró el impacto de las vulnerabilidades tomando en cuenta las consecuencias y repercusiones en las operaciones, resultados que se muestran en la tabla 3.16.

Tabla 3.13 Criterios de evaluación de impacto

Activo Crítico	Criterios de evaluación de impacto		
	Alto	Medio	Bajo
Sistema Administrativo Financiero (SAF)	El sistema no será funcional, tendrá pérdida de datos o perderá fidelidad la información.	Los daños en sistema pueden reparar en el corto plazo.	Los daños son pocos significativos y no dañan la integridad del sistema.
Servicio de Internet	No se tiene servicio activo y es imposible la comunicación con el exterior	El servicio es intermitente y no es accesible para todos los usuarios	Hay problemas de acceso y caídas de servicio, pero este no es interrumpido.
Infraestructura de red	La red es inoperante y todo los servicios no están disponibles para ninguna persona en la institución	Existen problemas de red que puede resolverse a corto plazo	Existen puntos de red con problemas menores que son resueltos de inmediato
Personal de TI	Los servicios están inaccesibles, o no hay personal capacitado o autorizado para realizar las actividades de soporte.	Los servicios y acceso pueden recuperase a corto plazo por el personal existente.	Los daños son mínimos y no causan problemas de consideración.

Fuente: Elaboración propia a partir del grado de impacto del riesgo para FUSALMO

3.3.1.6 Probabilidad del riesgo (Incidencia).

De acuerdo a esta metodología, la probabilidad del riesgo debe interpretarse como la frecuencia de ocurrencia de los riesgos en la institución en estudio, por tanto no corresponde a una valoración matemática, sino a la frecuencia de incidencia del riesgo. De tal modo que, en la tabla 3.14 se muestra la probabilidad del riesgo en función de la frecuencia de ocurrencia del mismo.

Tabla 3.14 Criterios de evaluación de probabilidad de incidentes de seguridad

Valor	**Frecuencia de ocurrencia**
Alto	Más de 10 veces por año
Medio	De 2 a 9 veces por año
Bajo	Una vez por año

Fuente: Elaboración propia a partir de la probabilidad de incidentes de seguridad para FUSALMO

De acuerdo a esta escala y los antecedentes de la Institución en estudio, se valoró la probabilidad (Incidencia) de los riesgos que se muestran en la Tabla 3.16.

3.3.1.7 Valor cualitativo del riesgo.

La metodología establece que luego de analizar la probabilidad (Incidencia) de cada riesgo, se determina el Valor cualitativo del riesgo mediante una matriz de Probabilidad – Impacto (P-I) ya establecida. En la Tabla 3.15 se muestra la relación Probabilidad – Impacto en escala bajo, medio y alto.

Tabla 3.15: Relación P-I para determinar el valor cualitativo del riesgo

		Probabilidad (Incidencia)		
		Alto	**Medio**	**Bajo**
Impacto	**Alto**	Alto	Alto	Medio
	Medio	Alto	Medio	Bajo
	Bajo	Medio	Bajo	Bajo

Fuente: OCTAVE, 10.7 Incorporando la probabilidad en la mitigación del riesgo.

Es así como para determinar el Valor cualitativo del riesgo, éste resulta de la intersección de la valoración de impacto y la probabilidad (Incidencia) asignada a cada riesgo en los activos críticos, mediante un resultado en escala bajo, medio o alto; lo cual determinará las consideraciones para la mitigación de riesgos.

Finalmente, en la tabla 3.16 se muestra en forma integrada la identificación de activos críticos, los requerimientos de seguridad de estos activos en función de su disponibilidad, confidencialidad e integridad; además las amenazas, las vulnerabilidades asociadas a estas amenazas, los riesgos y su impacto e incidencia.

Como resultado del análisis de riesgo; se identificaron 5 riesgos con valoración baja, 11 con valoración media y 5 con valoración alta, tal como se muestra en la figura 3.5; los cuales brindan pautas a la Institución en relación a los riesgos que es necesario controlar.

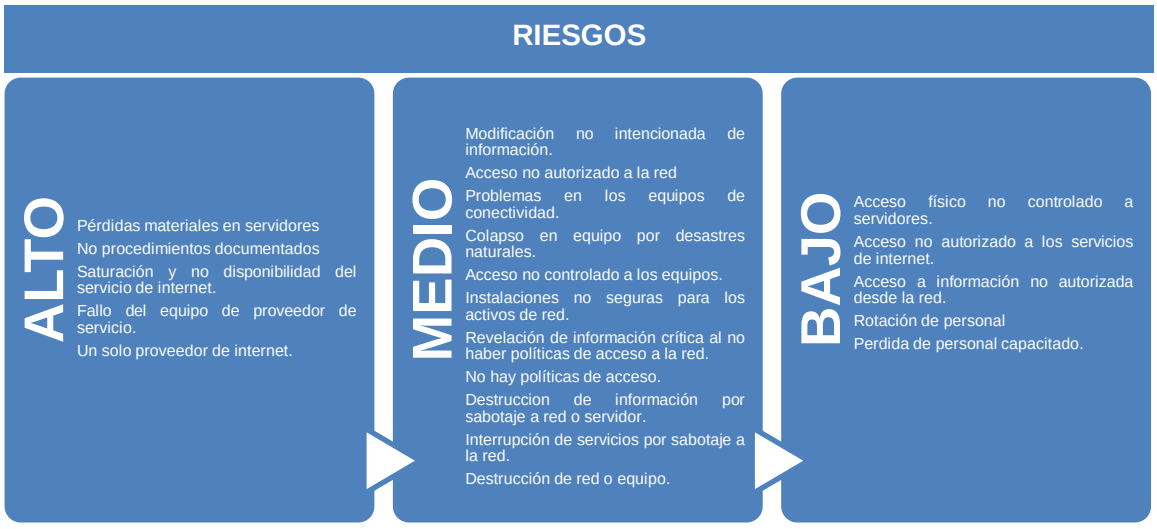


Figura 3.5 Identificación de riesgos para FUSALMO.

Tabla 3.16 Resultados de la valoración de riesgos FUSALMO

ACTIVO CRÍTICO	DESCRIPCIÓN	REQUERIMIENTOS DE SEGURIDAD PARA LOS ACTIVOS CRITICOS			TIPOS DE AMENAZA	VULNERABILIDADES	RIESGO	IMPACTO	PROBABILIDAD (INCIDENCIA)	VALOR CUALITATIVO DEL RIESGO
		DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD						
Sistema Administrativo Financiero (SAF)	Sistema para el registro contable y financiero. Sistema crítico donde se administra información confidencial, capaz de interrumpir las operaciones comerciales en caso de pérdida o manipulación.	Eficiencia en el procesamiento de la información. Disponibilidad de la información para usuarios autorizados 24/7	Autenticación de usuarios para acceder a la información. Sesiones de acceso con advertencia de seguridad Medidas de protección de sesión de usuario ausente.	Advertencia de seguridad en la modificación de información por usuarios autorizados.	Acciones humanas relacionada con el acceso físico	Acceso físico no controlado a servidores.	Modificación de información crítica	**Medio**	**Bajo**	**Bajo**
						Pérdidas materiales por manipulación de equipos en área de servidores.	Interrupción del acceso	**Alto**	**Medio**	**Alto**
					Acciones humanas relacionadas con el acceso de red	Modificación no intencionada de la información.	Interrupción del acceso	**Medio**	**Medio**	**Medio**
						Personal no autorizado puede tener acceso a la red.	Modificación de información crítica	**Alto**	**Bajo**	**Medio**
					Otros problemas	No existe procedimiento documentado de Back up del área contable o aplicaciones.	Revelación de información crítica	**Medio**	**Alto**	**Alto**
Servicio de Internet	Servicio externo para todos los clientes y colaboradores. Servicio crítico para los objetivos educativos y para las operaciones de sistemas internos.	Monitoreo permanente del servicio del proveedor. Disponibilidad para usuarios autorizados 24/7. Eficiencia en el tráfico de información.	Autenticación de clientes para el acceso a correo institucional y sesiones de usuario. Protección de datos y cuentas de usuario.	Restricción de acceso según política Aplicativos de SAF y correo electrónico deberán viajar en forma segura, mediante un SSL(security socket layer)	Acciones humanas relacionada con el acceso físico	Accesos no autorizados a la red	Interrupción del acceso	**Bajo**	**Medio**	**Bajo**
					Problemas en los sistemas	Problemas o fallas en los equipos responsables de la conectividad.	Interrupción del acceso	**Medio**	**Medio**	**Medio**
						Saturación del servicio y no disponibilidad	Interrupción del acceso	**Alto**	**Medio**	**Alto**
					Otros problemas	Colapso en los equipos responsables de la conectividad como resultado de desastres naturales.	Interrupción del acceso	**Alto**	**Bajo**	**Medio**

ACTIVO CRÍTICO	DESCRIPCIÓN	REQUERIMIENTOS DE SEGURIDAD PARA LOS ACTIVOS CRITICOS			TIPOS DE AMENAZA	VULNERABILIDADES	RIESGO	IMPACTO	PROBABILIDAD (INCIDENCIA)	VALOR CUALITATIVO DEL RIESGO
		DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD						
Servicio de Internet	Servicio externo para todos los clientes y colaboradores. Servicio crítico para los objetivos educativos y para las operaciones de sistemas internos.	Monitoreo permanente del servicio del proveedor. Disponibilidad para usuarios autorizados 24/7. Eficiencia en el tráfico de información.	Autenticación de clientes para el acceso a correo institucional y sesiones de usuario. Protección de datos y cuentas de usuario.	Restricción de acceso según política Aplicativos de SAF y correo electrónico deberán viajar en forma segura, mediante un SSL(security socket layer)	Otros problemas (Continuación)	Fallo de equipo del proveedor del servicio.	Interrupción del acceso	**Alto**	**Medio**	**Alto**
						Un solo proveedor del servicio no calificado por la Fundación.	Interrupción del acceso	**Alto**	**Alto**	**Alto**
Infraestructura de red	Comprende los dispositivos que permiten el funcionamiento de la red (routers, cables, servidores, switches, etc.) y transmisión y direccionamiento de información	Completa disponibilidad de todos los puntos de la infraestructura para la comunicación de información. Disponibilidad del 100% 24/7.	Restricción de acceso a terminales o personal no autorizado. Evitar manipulación no autorizada de los equipos mediante protocolos seguros para el acceso a los sistemas de administración de estos.	Política de respaldo de configuraciones Políticas de protección de los activos .	Acciones humanas relacionadas con el acceso físico	Acceso no controlado a los equipos.	Destrucción/Pérdida	**Medio**	**Medio**	**Medio**
						Instalaciones físicas no seguras para los activos.	Destrucción/Pérdida	**Alto**	**Bajo**	**Medio**
					Acciones humanas relacionadas con el acceso de red	Acceso a información no autorizada.	Revelación de información crítica	**Medio**	**Bajo**	**Bajo**
					Otros problemas	No existe una política de acceso a la red.	Revelación de información crítica	**Medio**	**Medio**	**Medio**
							Interrupción del acceso	**Medio**	**Medio**	**Medio**
Personal de TI	Es el Recurso Humano que brinda soporte al equipo y a las aplicaciones.	Personal capacitado para dar soporte de TI disponible al ser requerido	Políticas de seguridad para garantizar el manejo de la información. Aplicación de estándares de servicio	Personal autorizado para cada área informática	Acciones humanas relacionadas con el acceso físico	Sabotaje a red o servidor	Destrucción de información.	**Alto**	**Bajo**	**Medio**
							Interrupción de servicios	**Alto**	**Bajo**	**Medio**
					Acciones humanas relacionadas con el acceso de red	Destrucción de red o equipo	Interrupción del acceso	**Alto**	**Bajo**	**Medio**
					Otros problemas	Rotación de personal y pérdida de personal capacitado	Interrupción del acceso	**Medio**	**Bajo**	**Bajo**
							Destrucción de información.	**Medio**	**Bajo**	**Bajo**

Fuente: Elaboración a partir de la metodología de análisis OCTAVE y resultados del diagnóstico en FUSALMO

3.4 Análisis económico de los incidentes de seguridad

Al analizar económicamente los incidentes de seguridad, se tomó de referencia un incidente de seguridad identificado y reconocido institucionalmente desde la alta gerencia, el cual consistió en pérdida de información confidencial del área financiera, debido a faltas de carácter humano y manipulación de servidores. Este antecedente permitió aproximar los costos en recurso humano involucrado, materiales y costos directos o indirectos no cuantificables por su naturaleza, a fin de determinar el monto económico que representa para la Institución, las pérdidas por incidentes de seguridad.

Este incidente significó a la Fundación:

a) Pérdidas económicas
b) Asignación de recurso humano dedicado a la recuperación de información.
c) Interrupción en la continuidad del negocio
d) Inversión en materiales para la restauración
e) Horas de trabajo-persona extra para el registro de la información.
f) Un aproximado de tres meses de trabajo en la recuperación de la información.

Este incidente dejó en evidencia:

a) La necesidad de procedimientos para el resguardo de la información crítica y confidencial.
b) Necesidad de aislamiento de las instalaciones de almacenamiento y procesamiento de información crítica y confidencial.
c) Necesidad de realizar respaldos de información de las áreas críticas en forma periódica y frecuente; entre otros.

Es así como la Institución en respuesta a la situación, se vio en la necesidad de invertir horas de trabajo y equipo para poder recuperar el respaldo de información según el detalle de la Tabla 3.17.

Tabla 3.17 Análisis económico del incidente descrito

Personal Asignado		**Horas - persona**	**Costo Promedio ($)**
Gerencia Contable	1	40	$ 480.00
Auxiliar Contable	1	40	$ 480.00
Gerente de TI	1	20	$ 240.00
Personal de Soporte	2	100	$ 800.00
Sub Total Horas-Persona		200	**$ 2000.00**
		Costos Materiales	**$ 400.00**
		Total (Sub Total Horas-Persona + Costos Materiales)	**$ 2,400.00**

Fuente: Elaboración propia a partir de datos proporcionados por la Gerencia de Tecnología e Innovación.

Se involucraron en el proceso 3 empleados administrativos y 2 de soporte, realizando un total de 200 horas-persona, sumado a la inversión en bienes materiales por un monto total de $ 2,400.00.

Dentro de las pérdidas no cuantificables se tienen:

a) Retraso en pagos a proveedores y salarios del personal.
b) Retrasos en cobros.
c) Pérdida de información contable para ejecución de auditorías financieras.
d) Riesgo de pérdidas en concursos de proyectos debido a no disponibilidad de la información contable actualizada y de manera inmediata.
e) Otros costos indirectos no definidos.

Para el cálculo de los costos indirectos relacionados al incidente, estos se determinan en función de los costos directos aplicando el método de Heinrich[10] mediante la siguiente función:

Ci = a x Cd

Donde:

Ci = Costos indirectos

a = en un valor corriente equivalente a 4

Cd = Costos directos

Sustituyendo el valor de “a” la expresión es la siguiente:

Ci = 4 x Cd (1)

Partiendo que el costo total (CT) se define con la siguiente expresión:

CT = Cd + Ci (2)

Sustituyendo la expresión “1” en la de costos totales da como resultado:

CT = 5 x Cd (Costos totales sería el quíntuple de los costos directos)

Aplicando la expresión anterior al incidente de seguridad, donde el costo directo fue de $2,400 tenemos que para FUSALMO el costo total represento un monto de $ 12,000.00.

Por tanto, implementar un SGSI, representa una alternativa viable para la Institución en la prevención de incidentes como el detallado anteriormente, mismo que pudo ser evitado con las debidas políticas, procedimientos y medidas de seguridad física pertinentes al caso.

[10] Método para estimación de costos indirectos para incidentes a partir de la determinación de los costos directos diseñado por Heinrich Himmler (Mayo 1,945).

Considerando lo anterior y una vez analizadas las condiciones de la Institución, se realizó una investigación para identificar a otras instituciones que operan en el país y que ya han implementado un SGSI, para así retomar sus experiencias en el desarrollo de este modelo. Para tal propósito, se utilizó la herramienta Benchmarking aplicada a dos Instituciones identificadas con éstos requerimientos, siendo estas el Banco Central de Reserva y TACA Airlines El Salvador.

3.5 Benchmarking – Caso de estudio Banco Central de Reserva de El Salvador y TACA Airlines El Salvador.

El Benchmarking se presenta como una herramienta útil en la innovación dentro de una organización, permitiendo realizar mejoras en sus procesos y excelencia empresarial retomando experiencias del mercado. Este se define como un proceso sistemático y continuo para evaluar productos y/o servicios, así como procesos de trabajo de otras organizaciones que son reconocidas como practicantes del mismo, con el objetivo de lograr implementaciones y mejoras en la organización.

En nuestro país se identificó a las empresas TACA Airlines y el Banco Central de Reserva de El Salvador (BCR) por su experiencia en la implementación de un SGSI basado en el estándar ISO 27001:2005.

3.5.1 Objetivo del benchmarking

Identificar los factores claves de éxito que le permitieron al BCR y TACA, implementar los controles especificados en la norma ISO/IEC 27001:2005, para capitalizar su experiencia en relación al estado actual de la gestión de seguridad de la información en FUSALMO.

3.5.2 Metodología del benchmarking

Para la realización del Benchmarking se toma como base el tipo funcional, el cual permite comparar con organizaciones reconocidas, teniendo lo más avanzado en productos/servicios en proceso. Este proceso es desarrollado de la siguiente manera:

a) Identificar las necesidades específicas de la información.
b) Identificar los socios del benchmarking, detectando las mejores prácticas en las organizaciones.
c) Recopilar la información y presentar resultados del análisis.

3.5.3 Casos de Estudio TACA Airlines – Banco Central de Reserva de El Salvador

Ambas instituciones en estudio cuentan con un factor común, donde su trayectoria y experiencia de más de 77 años desde su fundación ha implicado una modernización y mejora continua de sus procesos, así como su incorporación en la era de las Tecnologías de la Información y las Comunicaciones (TIC´s). A continuación se detallan los factores clave de éxito y cambios relevantes para cada una de estas Instituciones.

3.5.3.1 Factores clave de éxito para el BCR

A continuación, en la tabla 3.18 se muestran los aspectos cualitativos de éxito para el Banco Central de Reserva en la implementación del SGSI según el estándar ISO 27001:2005.

Tabla 3.18 Factores claves de éxito para el Banco Central de Reserva en la implementación del SGSI según el estándar ISO 27001:2005.

Antecedentes	Factores Claves de Éxito BCR	Cambios Relevantes BCR
Carencia de un control constante e imparcial sobre el ejercicio de los procesos informáticos dentro de la organización.	Realización de un diagnóstico y análisis de riesgos. Reorganización a nivel del departamento de informática que permite el surgimiento de un comité de seguridad de la información con funciones claves y opinión objetiva sobre los procesos y políticas.	a) La creación de un comité de seguridad de la información que se encarga de velar el conveniente y correcto funcionamiento de la información conforme a las normas y políticas adoptadas. b) A través de diversos mecanismos y políticas dictadas como cultura organizacional se pretende asegurar la integridad, seguridad y disponibilidad de la información. c) Instalación de dispositivos de seguridad (firewall) que permitan la segura manipulación de la información desde perímetros externos hasta el manejo interno de datos y documentos específicos, a través del filtrado de la información. d) Análisis de las brechas entre el estado actual de la seguridad y las mejores prácticas de seguridad. e) Diseño y documentación de políticas, procedimientos y soluciones para asegurar la protección. f) Administración y soporte del programa de seguridad para servir a las metas de la organización y garantizar la continuidad del negocio.
Los mecanismos de seguridad utilizados eran insuficientes, debido que desconocían con detalle los riesgos que enfrentaban.	Definieron y tropicalizaron la mejor metodología de seguridad de información basados en las necesidades de la institución. Modificaron estructura informática y colocaron firewall[11] cada vez más específicos para un mejor control. Implementaron Data Lost Prevention.[12] Definieron la figura de un vigilante constante de los sistemas informáticos para toda la organización que está alerta de las anomalías presentes. Se aplica metodologías para análisis de riesgos tales como: OCTAVE[13], MAGERIT[14], COBIT[15], ITIL[16]; con base a estas, tropicalizaron su propia metodología de análisis de riesgos en base a las necesidades propias de la institución.	
El recurso humano no conocía sobre los límites establecidos en la manipulación de la información	Se crea toda una cultura de seguridad de la información que involucra a todos los empleados como entes activos en la transferencia de datos. Como parte de su mapa de proceso, la educación es clave para que la organización comprenda las mejores prácticas de seguridad y opciones más recomendadas en tecnología	

Fuente: Elaboración propia a partir de investigación realizada con representante de Seguridad de la Información del BCR

[11] Sistema de defensa (hardware y software) basado en que el tráfico de entrada o salida a la red pasa por un sistema de seguridad que autoriza, deniega y registra todo evento en función de una política de seguridad; controlando la comunicación interna y externa de la red.
[12] Herramienta que identifica, supervisa y protege la información confidencial almacenada, en uso o en tránsito dentro de la red, estaciones de trabajo o dispositivos móviles.
[13] OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation
[14] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
[15] COBIT: Control Objective for Information and Related Technology
[16] ITIL: Information Technology Infrestructure Library

3.5.3.2 Conclusiones del proceso en el BCR

a) La constante preparación y antelación de posibles riesgos, prácticamente ha vuelto nulo en número de incidentes informáticos en la organización y pérdida de información.
b) La educación en seguridad de la información y el involucramiento de empleados ha llevado a crear una verdadera cultura en seguridad de la información, que les permite contar con Recurso Humano de valor para la ejecución de los procesos en seguridad.
c) Lo referente a seguridad de la información, convierte al Departamento de Informática en un socio estratégico fuerte, que provee y manipula información basado en las mejores prácticas.
d) Internacionalmente la institución está respaldada, con un sistema de seguridad de la información que lo convierten en un aliado confiable y atractivo para organizaciones y clientes externos.

3.5.3.3 Factores clave de éxito para TACA Airlines

En la tabla 3.19 se muestran los factores clave de éxito identificados para la Institución en la implementación del SGSI según el estándar ISO 27001:2005.

Tabla 3.19 Factores claves de éxito para TACA en la implementación del SGSI según el estándar ISO 27001:2005.

Antecedentes	Factores Claves de Éxito TACA	Cambios Relevantes TACA
Ataques a la información y sistemas informáticos desde Internet.	Implementación de Firewalls e Intrusión Prevention Systems	a) Implementación de un sistema de seguridad en profundidad o en capas, el cual permite tener mecanismos de diferentes partes o ubicaciones. b) Creación de un comité de seguridad de la información. c) Implementación en la base de datos de configuraciones, roles y permisos para proteger la información. d) Capacitación al personal de la Dirección de Tecnología de la Información, en los nuevos sistemas y procedimientos. e) Implementación de marcos y regulaciones como SOX (Ley Sarbanes-Oxley), PCI (Peripheral Component Interconnect) y el estándar de Star Alliance f) Diseño de los procedimientos aplicables acorde al estándar ISO/IEC 27001:2005
Pérdida de la confidencialidad de la información sensible como tarjetas de crédito.	Implementación de cifrado a nivel de datos y SSL (Secure Socket Layer[17]) o HTTPS (Hyper Text Transfer protocol Secure[18]) en el transporte	
Pérdida de la disponibilidad de la información.	Implementación de mecanismos que eviten DoS (Denegación de Servicio) a nivel perimetral configurando directivas o políticas en IPS (Inventory of Programs and Services), filtrado de contenido, y bloqueo de tráfico con Firewalls.	
Amenazas de Virus y Gusanos que podrían afectar el funcionamiento de Servidores y estaciones de trabajo	Configuración y actualización periódica de Antivirus	
Ataques a los sistemas informáticos desde el exterior (internet) aprovechando fallos o vulnerabilidades en aplicaciones.	Actualización o parcheo periódico del sistema operativo y aplicaciones afectadas	
Robo de información	Bloqueo de dispositivos removibles con aplicaciones como Device Control para evitar fuga de datos a través de USB, CD, DVS, etc.	
Acceso y modificación no autorizada de la información	Implementación de Controles de acceso, definiciones de roles o perfiles a nivel de sistema operativo, aplicaciones, bases de datos, etc	
Fraude	Cifrado de información relacionada con tarjetas de créditos, a nivel de base de datos con AS256 y a través de la red uso de protocolo https.	

Fuente: Elaboración propia a partir de investigación realizada con representante de Seguridad de la Información de TACA

[17] Sistema de comunicación encriptada en internet que proporciona privacidad a los datos y mensajes, además permite autenticar datos enviados.
[18] Combinación de protocolo HTTP y protocolos criptográficos; empleado para lograr conexiones más seguras en la web, de modo que la información es cifrada.

3.5.3.4 Conclusiones del proceso en TACA

a) La implementación de los controles en los sistemas, permite proteger la integridad, disponibilidad y confiabilidad de la información, brindando mayor seguridad en caso que un atacante desee alterar, eliminar o robar la información de TACA.
b) La implementación del estándar ISO/IEC 27001:2005, aporta gran ayuda al cumplimiento de las regulaciones exigidas y así poder cotizar en la bolsa o ingresar alianzas mundiales.
c) La implementación del sistema y mecanismos, para proteger la información contribuye a que la empresa tenga una imagen seria y confiable.
d) El implementar mecanismos, sistemas, políticas y procedimientos para salvaguardar la información, contribuye a la productividad de la empresa, ya que gracias a la implementación de estos, se pretende mitigar ciertos problemas que potencialmente se podrían dar en ausencia de los mismos.

3.5.4 Análisis Comparativo con FUSALMO.

A continuación, en las tablas 3.20 y 3.21 se detalla la relación entre los factores claves de éxitos de las dos organizaciones seleccionadas en la realización del benchmarking con respecto a FUSALMO.

Tabla 3.20 Análisis comparativo Banco Central de Reserva de El Salvador - FUSALMO

No	Factores Claves de Éxito BCR	FUSALMO
1	Reorganización a nivel del departamento de informática que permite el surgimiento de un comité de seguridad de la información con funciones estratégicas y opinión objetiva sobre los procesos y políticas.	Actualmente, cuenta con una gerencia de Tecnología e Innovación, pero carecen de un comité de seguridad de la información.

No	Factores Claves de Éxito BCR	FUSALMO
2	Definieron y tropicalizaron la mejor metodología de seguridad de información basados en las necesidades de la institución.	Aun no se tiene definido alguna metodología para aplicar el estándar ISO/IEC 27001:2005.
3	Modificaron estructura informática y colocaron firewall cada vez más específicos para un mejor control.	Actualmente cuentan con la aplicación Firewall.
4	Implementaron Data Lost Prevention	No tienen esta aplicación.
5	Definieron la figura de un vigilante constante de los sistemas informáticos para toda la organización que está alerta de las anomalías presentes	Cuentan con alertas definidas por el Firewall.
6	Se crea toda una cultura de seguridad de la información que involucra a todos los empleados como entes activos en la transferencia de datos.	Actualmente no se cuenta con una divulgación de algún plan que involucre la seguridad de la información.
7	Como parte de su mapa de proceso, la educación es clave para que la organización comprenda las mejores prácticas de seguridad y opciones más reomendadas en tecnología	Actualmente no cuenta con algún plan de buenas prácticas de seguridad.

Fuente: Elaboración propia a partir de investigación realizada con representante de Seguridad de la Información del BCR e investigación en FUSALMO

Tabla 3.21 Análisis comparativo TACA – FUSALMO

No	Factores Claves de Éxito TACA	FUSALMO
1	Implementación de Firewalls e Intrusion Prevention Systems	Actualmente cuentan con la aplicación Firewall, no cuentan con Intrusion Prevention Systems.
2	Implementación de cifrado a nivel de datos y SSL o HTTPS en el transporte	No cuentan con este sistema.
3	Implementación de mecanismos que eviten DoS (Denegación de Servicio) a nivel perimetral configurando directivas o políticas en IPS, filtrado de contenido, y bloqueo de tráfico con Firewalls.	Cuentan con filtrados de contenidos, bloqueo de tráfico con Firewalls.
4	Configuración y actualización periódica de Antivirus	No cuentan con un programa de actualización de Antivirus.

No	Factores Claves de Éxito TACA	FUSALMO
5	Actualización o parcheo periódico del sistema operativo y aplicaciones afectadas.	No tienen un programa de actualización y parcheos periódicas.
6	Bloqueo de dispositivos removibles con aplicaciones como Device Control para evitar fuga de datos a través de USB, CD, DVS, etc.	Cuentan con bloqueo de equipos, de acuerdo a las políticas definidas.
7	Implementación de Controles de acceso, definiciones de roles o perfiles a nivel de sistema operativo, aplicaciones, bases de datos, etc	Cuentan con control de usuarios de acuerdo a los perfiles de estos.

Fuente: Elaboración propia a partir de investigación realizada con representante de Seguridad de la Información de TACA e investigación en FUSALMO

3.6 Resumen de resultados obtenidos con las herramientas de diagnóstico

En la tabla 3.22, se muestra un resumen de los aportes de cada una de las herramientas de análisis en el desarrollo del diagnóstico de la Institución, las cuales fueron complementarias entre sí y al mismo tiempo destacaron factores críticos para la misma. Los hallazgos se presentan en forma de Fortalezas y Debilidades desde la perspectiva de requerimientos del estándar internacional. Algunas de las fortalezas señaladas no están en el marco de requerimientos del estándar, pero se destacan como iniciativas de la Institución.

A nivel general se puede afirmar que la Fundación afronta muchas debilidades en relación a la seguridad de la información, por lo que los esfuerzos se focalizaron en identificar los aspectos críticos que deberán incorporarse en el modelo de SGSI para FUSALMO.

Tabla 3.22 Resultados de aplicación de herramientas de análisis

No.	Herramienta diagnóstica aplicada	Resultados	
		Fortaleza	**Debilidad**
1	Entrevista dirigida a: a) Dirección Ejecutiva. b) Gerencia Recursos humanos. c) Coordinación de recursos tecnológicos. d) Gerencia de Tecnología e innovación. e) Gerencia de Finanzas y Recaudación de fondos. f) Coordinación de mantenimiento	a. Se tiene implementado un respaldo de la información (back up) para el área financiera y contable, este se realiza semanalmente. b. Cuentan con un registro de asignación de equipos a los colaboradores. c. Cuentan con un sistema de seguridad de firewall (bloqueo de contenido perimetral). d. Cuentan con un control de usuarios externos en caso de capacitación. e. Emisión de reportes mensuales para medir la productividad de la personas y tener control de las páginas de internet que visitan, esto a nivel de gerencias y coordinadores. f. Cuentan con un control de ingresos de red para máquinas que no pertenecen a FUSALMO. g. Cuentan con invitaciones de talleres para seguridad de la información a nivel de educadores. h. Tienen cuentas asignadas a invitados para usos de los activos en los centros de cómputo, éstas poseen restricciones de acceso. i. Cuentan con un Reglamento de Usuarios (Área Educativa) j. Cuentan con acceso restringido a los servidores. Solamente dos personas tiene acceso autorizado a los servidores. k. Cuentan con una nomenclatura de	a. No cuentan con un sistema de seguridad de la información para el resto de la organización. b. No cuenta con un responsable de la seguridad de la información. c. No cuenta con procedimiento documentado de respaldo de la información. d. No cuentan con acuerdos de confiabilidad. e. No cuentan con un plan de revisión/verificación constante de los equipos asignados a los colaboradores. f. No cuentan con auditorias de software y sistemas a nivel interno. g. No cuentan con una política y procedimiento documentado de reporte de incidentes. h. No cuentan con un diseño apropiado para los equipos de cómputo que garantice la seguridad de éstos. i. No cuentan con un procedimiento documentado para dar de baja a un equipo. j. No cuentan con una nomenclatura de clasificación de la información por niveles de seguridad. k. No existen mecanismos de divulgación de cambios en las políticas de TI. l. No cuentan con un modelo de buenas prácticas de uso de la capacidad de almacenamiento de la información.

No.	Herramienta diagnóstica aplicada	Resultados	
		Fortaleza	**Debilidad**
	Entrevista dirigida a: a) Dirección Ejecutiva. b) Gerencia Recursos humanos. c) Coordinación de recursos tecnológicos. d) Gerencia de Tecnología e innovación. e) Gerencia de Finanzas y Recaudación de fondos.	almacenamiento de la información (nombre y fecha). l. Cuentan con alertas de penetración a la red de información. m. Cuentan con un monitoreo de banda ancha. n. Firma de contrato con proveedores de internet. o. Cuentan con bloqueo del código móvil. p. Cuentan con pruebas de nuevos sistemas por parte de usuarios. q. La red está configurada de acuerdo al estándar definido. r. Cuentan con un sistema informático para el manejo de la información, necesaria para el reclutamiento de personal. s. Existe un seguimiento y verificación de los antecedentes de las personas en fase de contratación a través de un formato escrito. t. El contrato de trabajo incluye una cláusula sobre confidencialidad de la información. u. Al finalizar un contrato laboral, a través del "finiquito" por medio del jefe inmediato, el personal hace entrega oficial de los bienes físicos propiedad de FUSALMO y de la información archivada en los equipos. v. Se conforma un grupo de trabajo para la elaboración y revisión de procedimientos del área de TI, dirigido por el gerente de TI y con VoBo de la Dirección ejecutiva. w. Los procedimientos se revisan con frecuencia	m. No se cuenta con un procedimiento documentado de solicitud de software y licencias de estos. n. No cuentan con un sistema de intranet para las áreas de FUSALMO donde se pueden publicar documentos. o. No cuentan con una certificación vigente de la red. p. Falta de registro escrito de la Política sobre el acceso y manejo de la información requerida para la contratación de personal (Curriculum Vitae, etc.) q. El sistema informático disponible para la manipulación de la información confidencial de RRHH está obsoleto y no precisa los requerimientos exigidos. r. No hay registro escrito sobre la política de control de verificación de antecedentes de las personas en fase de contratación. s. No cuentan con un protocolo oficial para realizar la inducción a personal nuevo o a terceras personas, para comunicar sobre las políticas de la Fundación y manejo específico de la información y confidencialidad. t. En caso de cambios en los sistemas informáticos o afines, no existe una retroalimentación sobre las modificaciones por parte de la Gerencia de Tecnología e Innovación.

No.	Herramienta diagnóstica aplicada	Resultados	
		Fortaleza	**Debilidad**
	Entrevista dirigida a: g) Dirección Ejecutiva. h) Gerencia Recursos humanos. i) Coordinación de recursos tecnológicos. j) Gerencia de Tecnología e innovación. k) Gerencia de Finanzas y Recaudación de fondos.	(al menos cada 3 meses) en el área de TI, aunque no están escritos, se revisa su ejecución. x. Existe una bitácora donde se registran las acciones desarrolladas y la ejecución de procedimientos de seguridad en el área de TI. y. Se tiene un Plan Anual Operativo (POA) para el área de TI y se somete a evaluaciones de seguimiento. Cada recurso tiene su planificación en relación a este POA. z. Los procedimientos de finalización de contrato se realizan en coordinación con RRHH y la jefatura inmediata: se eliminan cuenta de usuario de sistemas y correo electrónico. aa. En el área de TI se tiene documentos de la asignación de recursos de información (memorando) y los respectivos finiquitos. bb. Los cambios o renovación de tecnología se realizan mediante propuesta y justificación de necesidades y se realiza la gestión ante la Dirección Ejecutiva. cc. Se tiene un inventario actualizado y la respectiva asignación. dd. Se tienen medidas de seguridad física para el acceso de usuarios a las instalaciones, los estudiantes necesitan carnet para entrar a las instalaciones. ee. Las sesiones de las máquinas cuentan con privilegios de administrador.	u. No se cuenta con un procedimiento sancionatorio en caso de que algún empleado infrinja la cláusula de confidencialidad de la información definida en el contrato de trabajo. v. En caso de culminación de contrato laboral, el personal de Tecnología e Innovación, no verifica los datos entregados en el respaldo (back up) por el personal. w. Hay procedimientos en el área de TI que se han implementado y deben mejorarse continuamente, sin embargo éstos no están documentados. x. No se tiene establecido una estrategia o política de seguridad. y. No se documenta la revisión de procedimientos. z. Las acciones relacionadas con la finalización de contrato no se han establecido de manera estandarizada y quedan sujetas a la iniciativa del jefe de Recursos Humanos donde se genera la finalización de contrato. aa. No hay garantía de que los empleados no extraigan información de la organización. bb. No están registradas las recomendaciones a usuarios en cuanto al uso de equipos y restricciones de seguridad ya que estas se realizan en forma verbal. cc. No se tienen acuerdos de confidencialidad con el recurso humano involucrado con la

No.	Herramienta diagnóstica aplicada	Resultados	
		Fortaleza	**Debilidad**
		ff. La empresa Business Software Alliance (BSA) realiza auditorias eventuales de licenciamiento de software y solo se maneja software legal. gg. Se realizan pruebas piloto en la implementación de software nuevo. hh. Se han realizado mejoras en cuanto a limitar el acceso físico y virtual a los servidores.	información confidencial. dd. Se brindan recomendaciones no escritas a los docentes y consultores sobre la conducta y prácticas en las instalaciones. Al personal interno se le entrega el reglamento interno de trabajo ee. No se tiene un protocolo o procedimiento en casos de incidentes de seguridad, investigación de eventos, responsabilidades e implicaciones. ff. Se necesita formación del personal técnico en relación a la seguridad de la información (2 personas en el área de soporte y seguridad y 1 persona en desarrollo de software) gg. No se tiene sistema de monitoreo en los centros de cómputo. hh. Por falta de seguridad se han presentado casos extravío de hardware en las instalaciones de cómputo. ii. Se tienen debilidades en cuanto a prevención de riesgos ambientales en el área de servidores, no se tienen extintores, ni anclaje de mobiliario. jj. Se tiene una sola acometida para suministro de energía y no hay planta eléctrica interna de emergencia. kk. Poseen sistema de alarma centralizado para la infraestructura administrativa, sin incorporar área de servidores.

No.	Herramienta diagnóstica aplicada	Resultados	
		Fortaleza	**Debilidad**
2	Herramienta de valoración en base a requerimientos del estándar ISO/IEC 27001:2005 Herramienta de valoración en base a requerimientos del estándar ISO/IEC 27001:2005	a. Cuentan con inventario de los equipos y asignación de éstos, desde la contratación. b. Cuentan con mecanismos de investigación del perfil de los candidatos a contratar. c. Se han implementado medidas de garantía de la seguridad en la finalización del empleo. d. Cuentan con sistema contra incendios en algunas áreas claves del área administrativa. e. Cuentan con controles de uso de equipos fuera de las instalaciones y su disposición final. f. Se tiene bitácoras de los controles de cambios, en caso de pruebas de nuevos sistema se realizan de forma aislada y en periodos específicos. g. Monitoreo de la capacidad de los sistemas. h. Cuentan con procedimientos de respaldo en las áreas críticas, éste no está documentado. i. Cuenta con un proceso de medidas de almacenamiento de información por áreas. j. El acceso a los sistemas están protegidos por contraseña mediante autenticación de usuario.	a. No cuentan con una política de seguridad implementada ni definida. b. No se tiene documentado los accesos restringidos a áreas clave. c. No tienen procedimiento de acción disciplinaria en caso de que se tenga una violación de la seguridad de la información. d. Cuentan con deficiencia en el perímetro físico de las áreas de procesamiento de información especialmente en el área educativa. e. No cuentan con controles o auditorias sobre los servicios brindados por terceros. f. El proveedor de servicio de redes no ha sido calificado por la Fundación. g. No cuenta con políticas ni medidas de seguridad en relación al uso de medios extraíbles. h. No se ha identificado los requerimientos de seguridad para los sistemas nuevos o los ya existentes. i. No existe un procedimiento para reporte de incidentes, ni gestión de incidentes. j. No existen regulaciones o legislación definidas a las cuales dar cumplimiento.

No.	Herramienta diagnóstica aplicada	Resultados	
		Fortaleza	**Debilidad**
3	Esquema Tela de araña	Mediante los gráficos de tela de araña se identificaron las siguientes fortalezas por ámbito: a) Planeación y aceptación del sistema b) Responsabilidad por los activos c) Clasificación de la información: Finalización o cambio de empleo. d) Protección contra códigos maliciosos y móviles e) Control de acceso a sistemas operativos f) Control de acceso a redes g) Seguridad en procesos de desarrollo y soporte h) Cumplimiento de requerimientos legales i) Seguridad de archivos de sistema.	Las debilidades identificadas son las siguientes: a) Política de seguridad de la información b) Organización interna de la seguridad c) Gestión de la entrega de servicios a terceros. d) Control de acceso de aplicaciones e información. e) Monitoreo. f) Control de acceso para usuarios g) Gestión de incidentes y mejoras en la seguridad de la información. h) Requerimientos de seguridad de los sistemas de información y procesamiento correcto de las aplicaciones. i) Consideraciones de auditoría de los sistemas de información.
4	Análisis de riesgos	a) Se ha establecido una metodología para el análisis de riesgos. b) Se han identificado los activos críticos de la Institución, a fin de su protección e integridad.	a) Alto riesgo de pérdidas materiales en servidores. b) Procedimientos no documentados. c) Único proveedor de internet (No garantía por falla externa), posible interrupción del servicio. d) Riesgos de modificación no intencionada de la información. e) Riesgo de colapso de equipos en situaciones de desastres naturales. f) Instalaciones no seguras para los activos de red. g) Riesgo por destrucción de información en sabotaje de red o equipos. h) Riesgo de interrupción de servicios.

No.	Herramienta diagnóstica aplicada	Resultados	
		Fortaleza	**Debilidad**
5	Análisis económico de los incidentes de seguridad	a) Identificación de un incidente de seguridad, reconocido desde la alta gerencia. b) Reconocimiento de las consecuencias del incidente de seguridad y sus implicaciones. c) Implementación de algunas medidas de seguridad luego del incidente. d) Estimación de los costos asociados al incidente. e) Identificación de las pérdidas cuantificables y no cuantificables.	a) No existe un procedimiento para el seguimiento de incidentes de seguridad. b) No se ha documentado el incidente ni deducido responsabilidades. c) El incidente representó a la Institución al menos $2,400 USD en costos directos y un indeterminado valor en costos no cuantificables directamente relacionados con las operaciones de ésta. d) Las consecuencias del incidente perjudicaron a clientes internos como externos, así como el ambiente y relaciones laborales.

Fuente: Elaboración propia a partir de los resultados de la investigación realizada en FUSALMO.

3.7 Factores críticos para la Institución.

A partir de los resultados obtenidos a través de las herramientas de diagnóstico, análisis de riesgos, análisis económico de incidentes y benchmarking, se definen diez factores críticos para la Institución, los cuales se detallan a continuación.

a) Política de seguridad.

Actualmente la Institución carece de una política de seguridad integral de los activos informáticos que le permita administrar de manera eficiente los mismos. En caso de no tomar acciones concretas se ve expuesto a toma de decisiones ineficientes que provoquen aumentos en los costos operativos y financieros de la fundación y pongan en peligro las operaciones y la continuidad del negocio.

b) Organización de la seguridad de la información.

La ausencia de un registro escrito sobre el manejo de la información y las atribuciones de los usuarios sobre la misma, así como de un comité objetivo que vigile las prácticas de organización y seguridad de la información, genera una situación descontrolada que lleva a la improvisación en caso de incidentes o manejo inadecuado de la información. Al no realizar cambios a los procesos actuales, aumenta la probabilidad que haya un manejo ineficiente de los recursos a disposición, lo que se traduce en disminución de rentabilidad.

c) Compromiso de la dirección.

No se ha evidenciado un compromiso fiel por parte de la Junta Directiva y demás autoridades sobre el diseño e implementación de una política de seguridad de la información. Esto implica que carecen del aseguramiento de recursos adecuados para implementar y mantener las políticas de seguridad de la información. Concretamente si no hay respuesta de apoyo desde la alta Dirección, todo intento y esfuerzo realizado en la construcción de la cultura de seguridad será frustrado para la organización y traducido en desperdicio de recursos.

d) Procedimientos

La ausencia de procedimientos documentados orientados a salvaguardar la información, dificulta una cultura de protección de la información. Si la organización carece de estas prácticas, se corre el riesgo que la información sea accedida por cualquiera, ocasionando que esta sea alterada o eliminada.

e) Respaldo de la información

La Institución no posee procedimientos documentados para el respaldo de la información. El respaldo de los datos son una de las prácticas más importantes para cualquier entidad, esto se lleva a cabo con el fin de dar continuidad con las operaciones de la compañía en caso de desastres o pérdidas de información, lo que demanda un procedimiento para su respaldo y recuperación.

f) Control de acceso a aplicaciones e información.

La Institución no cuenta con una política para el acceso autorizado a aplicaciones e información; la ausencia de la misma implica que no existe un lineamiento institucional escrito para gestionar las restricciones de acceso a la información, esto a pesar de contar con medidas técnicas que restringen el acceso al usuario, no brindando respaldo y garantías al proceso de monitoreo, seguimiento y auditoría informática, así como en la gestión de incidentes de seguridad.

g) Monitoreo – Auditoria.

No se ha implementado un sistema de auditoría interna o externa a nivel informático, ni registros de las actividades propias o accesos no autorizados a los sistemas, aplicaciones o hardware; esta condición coloca a la Fundación en una situación de alta vulnerabilidad al no dar seguimiento a los riesgos que enfrenta, ni el registro de los mismos para la retroalimentación efectiva de las acciones de mejora, quedando expuesta a reincidencia de eventos de

seguridad, costos asociados a vulnerabilidad en la continuidad del negocio, no identificación de nuevos riesgos o vulnerabilidades, entre otros.

h) Acuerdo de confidencialidad.

La Institución no ha establecido el uso de acuerdos de confidencialidad con el personal clave involucrado en el acceso a la información; esto genera una vulnerabilidad en la protección de la seguridad de la información crítica por parte del recurso humano, lo cual repercute en deficiencias en la asignación de responsabilidad, vacíos en el registro de incidentes, deficiencias en la garantía de seguridad de los procedimientos en los sistemas, entre otros.

i) Reporte de incidentes.

No se ha definido ningún procedimiento para el reporte de incidentes de seguridad, esto dificulta una respuesta inmediata ante la eventualidad de un incidente, su investigación, responsabilidad, registro y valoración de nuevas amenazas; por lo que es inminente la definición e implementación de procedimientos de reporte de incidentes donde claramente se definan las condiciones, medios y responsabilidad para reporte del incidente, así como las medidas para la gestión de los mismos. Caso contrario, la organización al no documentar estos eventos, se vuelve más vulnerable a antiguas y nuevas amenazas y las implicaciones económicas y de continuidad del negocio que esto implica.

j) Continuidad del negocio

Siendo la continuidad del negocio una necesidad imprescindible de las organizaciones; la Institución no cuenta con planes que garanticen la continuidad del negocio ante eventos que amenacen la seguridad física o técnica, tales como desastres naturales o resultado de acciones intencionadas en las áreas críticas y por tanto sus operaciones están comprometidas ante este tipo de eventos.

3.8 Procedimientos críticos para la Institución.

Considerando lo antes expuesto, se identifican catorce procedimientos necesarios para la Institución, de los cuales tres de ellos se consideran críticos en el proceso de implantación del SGSI. Por tanto, estos tres procedimientos han sido diseñados y son parte de la propuesta de esta investigación, considerando en ello el compromiso que debe asumir la Fundación para con los resultados de ésta, su continuidad y seguimiento.

Los procedimientos críticos diseñados y que se presentan en el Manual de Políticas de Seguridad de la Información son los siguientes:

a) Procedimiento de copia de respaldo de información (back up)
b) Procedimiento de reporte y seguimiento de incidentes de seguridad
c) Procedimiento de Auditoria de los sistemas de información

En corresponsabilidad, la Institución deberá realizar el levantamiento de 11 procedimientos adicionales que complementan el Manual de Políticas de la Seguridad de la Información, los cuales se detallan a continuación:

a) Procedimiento de Control de registros.
b) Procedimiento de clasificación de activos de información
c) Procedimiento de control de cambios
d) Procedimiento de control de medios e información en transito
e) Procedimiento de Gestión de accesos
f) Procedimiento de selección y contratación de personal
g) Procedimiento de medidas disciplinarias
h) Procedimiento de finalización de contrato
i) Procedimiento de no conformidades
j) Procedimiento de acciones correctivas y preventivas
k) Procedimiento de control de documentos.

CAPÍTULO IV. PROPUESTA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El modelo de sistema de gestión de seguridad de la información para la Institución incluye el diagnóstico en función de los requerimientos del estándar internacional, la metodología del análisis de riesgo y su correspondiente desarrollo, el establecimiento de los factores críticos, el plan y estrategias de implementación para la misma, recomendaciones, así como el Manual de políticas de seguridad de la información, este último disponible como Anexo III de este documento.

Por tanto, la implementación de este sistema requiere de un plan considerando todas sus fases hasta la certificación internacional, tal como se plantea a continuación.

4.1 Plan de implementación

El plan de implementación del SGSI contempla cinco etapas orientadas hacia una organización, delegación, ejecución y control de los procesos y actividades específicas de la Institución, tal como se detallan a continuación:

Etapa 1. Presentación del proyecto a Dirección Ejecutiva y Gerencias de la Fundación; actividad contemplada como responsabilidad del equipo de investigación a fin de comunicar y actualizar a la institución sobre la propuesta del Sistema de Gestión de Seguridad de la Información, tomando en cuenta a las Gerencias involucradas en la implementación del mismo.

Etapa 2. Conformación del Comité de Seguridad de la Información; el cual deberá estar conformado por un grupo de conocedores en el tema, que puedan emitir juicios y colaborar en la coordinación general. El propósito consiste en definir responsabilidad en la implementación, monitoreo, control y seguimiento del SGSI. Además de conformar el comité de seguridad, se deberá realizar capacitación al

mismo en relación a la metodología de adopción del sistema, requerimientos y etapas.

Etapa 3. Implementación del Sistema de Gestión de Seguridad de la Información. Comprende la divulgación y capacitación acerca del manual de Políticas y del SGSI a todos los niveles de la Fundación. En esta etapa se pretende sensibilizar a todo el personal acerca de las políticas y su impacto organizacional. Al mismo tiempo debe realizarse el levantamiento de procedimientos a fin de establecer la documentación del sistema de gestión.

Etapa 4. Evaluación del Desarrollo del Sistema. En esta etapa se define un proceso constante de mejora continua, que permita verificar el cumplimiento actual de requisitos y garantizar las mejores prácticas de seguridad de la información de manera permanente; para ello se debe realizar un proceso de auditoría interna y como resultado de ello la ejecución de acciones correctivas y no conformidades.

Etapa 5. Certificación del Sistema de Gestión de la Seguridad de la Información. En esta se pretende la certificación del sistema por una entidad externa certificada por la Organización Internacional de Normalización (Siglas en Ingles ISO).

En la tabla 4.1 se presenta el plan de implementación del SGSI, identificando las estrategias y fases que deberá desarrollar la Institución y en la tabla 4.2 se muestra el cronograma para su ejecución.

Tabla 4.1 PLAN DE IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

ACTIVIDADES DE IMPLEMENTACIÓN	RESPONSABLE	OBJETIVO	ESTRATEGIA	DOCUMENTACIÓN
Etapa 1: Presentación del proyecto a Dirección Ejecutiva y Gerencias de la Fundación				
Presentación del proyecto, diagnóstico y resultados a Dirección Ejecutiva y Gerencias	Equipo de investigación	Comunicar el proceso de investigación realizado y generar iniciativas que lleven a la ejecución del proyecto	Reunión para presentación de proyecto	Tesis: Propuesta del Modelo de Gestión del Sistema de Seguridad informática estándar ISO NF 27001:2005 para FUSALMO
Etapa 2: Conformación del Comité de Seguridad de la Información				
Establecimiento del Comité de Seguridad de la Información	Dirección Ejecutiva	Definir responsabilidad en la implementación, monitoreo, control y seguimiento del SGSI	Reunión con Comité de Seguridad de la Información	Tesis: Propuesta del Modelo de Gestión del Sistema de Seguridad informática estándar ISO NF 27001:2005 para FUSALMO
Capacitación al Comité de Seguridad en relación al SGSI	Gerencia de Tecnología e Innovación	Presentar metodología de adopción del sistema, requerimientos y etapas.	Reunión con Comité de Seguridad de la Información	SGSI
Etapa 3: Implementación del Sistema de Gestión de Seguridad de la Información				
Divulgación y capacitación acerca del Manual de Políticas y del SGSI a todos los niveles de la Fundación	Comité de Seguridad de la Información	Capacitar a todo el personal acerca de la Política y su impacto organizacional	Reunión con Gerencias y Jefaturas y miembros	Manual de Políticas de Seguridad de la Información Estándar ISO/IEC27001:2005 para FUSALMO

ACTIVIDADES DE IMPLEMENTACIÓN	RESPONSABLE	OBJETIVO	ESTRATEGIA	DOCUMENTACIÓN
Levantamiento de procedimientos y registros.	Comité de Seguridad de la información y otros vinculados a procesos	Integrar las funciones del personal	Instrucción y revisión de procedimientos de acuerdo al estándar indicado en política	Procesos y registros del Sistema
Etapa 4: Evaluación del Desarrollo del Sistema				
Planificación y ejecución de auditorías internas	Dirección Ejecutiva y Comité de Seguridad de la Información	Verificar el cumplimiento y mejoras del sistema.	Auditorías internas de supervisión	Procedimiento de auditoría interna y documentación del SGSI
Ejecución de acciones correctivas y no conformidades detectadas.	Comité de Seguridad de la Información		Revisión de resultados de auditoria	Procedimiento de acciones correctivas y no conformidades
Identificación e implementación de mejora continua	Dirección Ejecutiva y Comité de Seguridad de la Información		Evaluación de mejoras	Plan de mejora
Etapa 5: Certificación del Sistema de Gestión de la Seguridad de la Información				
Auditoria interna del SGSI	Comité de Seguridad de la Información	Identificar debilidades en el SGSI	Auditoría interna	Procedimiento de auditoría interna y documentación del SGSI
Ejecución de acciones correctivas y no conformidades detectadas.	Comité de Seguridad de la Información, Gerencia de Tecnología e Innovación, Jefaturas y Dirección Ejecutiva	Resolver los hallazgos de auditoria interna	Ejecución de plan de solución a hallazgos	Procedimiento de acciones correctivas y no conformidades
Auditoría de certificación del SGSI	Ente de certificación	Obtener requerimiento oficial de certificación	Auditoría por el ente de certificación	Certificación del SGSI

Fuente: Elaboración propia a partir de resultados de la investigación

Tabla 4.2: CRONOGRAMA DE IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

ACTIVIDADES	MESES											
	1	2	3	4	5	6	7	8	9	10	11	12
Etapa 1: Presentación del proyecto a Dirección Ejecutiva y Gerencias de la Fundación												
Presentación del proyecto, diagnóstico y resultados a Dirección ejecutiva y Gerencias												
Etapa 2: Conformación del Comité de Seguridad de la Información												
Establecimiento del Comité de Seguridad de la Información												
Capacitación al Comité de Seguridad en relación al SGSI												
Etapa 3: Implementación del Sistema de Gestión de Seguridad de la Información												
Divulgación y concientización del acerca del Manual de Políticas y del SGSI a todos los niveles de la Fundación												
Levantamiento de procedimientos y registros.												
Etapa 4: Evaluación del Desarrollo del Sistema												
Planificación y ejecución de auditorías internas												
Ejecución de acciones correctivas y no conformidades detectadas.												
Identificación e implementación de mejora continua												
Etapa 5: Certificación del Sistema de Gestión de la Seguridad de la Información												
Auditoria interna del SGSI												
Ejecución de acciones correctivas y no conformidades detectadas.												
Auditoría de certificación del SGSI												

Fuente: Elaboración propia a partir de resultados de la investigación

4.2 Estrategias para la implementación

A partir del diagnóstico realizado y el análisis de riesgo, se definen las estrategias que dan respuesta a las debilidades identificadas y que permitirán a FUSALMO establecer el SGSI y los requerimientos de la seguridad de la información.

a) Capacitación en seguridad de la información

Es necesario desarrollar un plan de formación institucional en sensibilidad en el tema de seguridad de la información, así como también capacitación del área de TI, a fin de actualizarse en nuevos riesgos y metodologías para evaluación y mitigación del riesgo.

b) Seguridad física de los equipos

Es importante acondicionar las áreas donde se procesa información crítica acorde al ambiente y riesgos a que se exponen, a fin de salvaguardar los equipos y la información, es necesario prever las condiciones de desastre e incorporar medidas en caso de siniestros o desastres naturales.

c) Levantamiento de procedimientos

Es indispensable que FUSALMO realice un levantamiento de procedimientos en todas sus áreas, especialmente en TI a fin de proteger y garantizar la documentación y ejecución de procedimientos aceptados por la alta dirección y la correspondiente asignación de responsabilidad sobre los mismos.

d) Administración de la seguridad

La administración de la seguridad debe ser un proceso compartido por todos los miembros de la organización como partes interesadas en la seguridad y vigilantes de las buenas prácticas.

e) Planes de continuidad

Es indispensable establecer y revisar planes de continuidad ante desastres, a fin de garantizar la continuidad del negocio y la protección de los activos críticos de la Fundación, estos planes al mismo tiempo deben ser del conocimiento de los miembros de la organización, promoviendo una actitud favorable para su correcta ejecución.

f) Comité de seguridad de la información.

Establecimiento de un Comité de Seguridad de la Información, totalmente independiente al área de Tecnología e Innovación, actuando como ente rector vigila la garantía de seguridad en todos los procedimientos y la adopción de buenas prácticas.

g) Auditoría

Es indispensable implementar un sistema de auditoria informática con todos sus controles y procedimientos a fin de dar seguimiento a las acciones relacionadas con las operaciones y administración de la seguridad. Este sistema deberá implementarse una vez se hayan definido los controles y procedimientos documentados para la fundación.

4.3 Consideraciones al plan de implementación

A continuación se detallan algunas consideraciones a la definición del plan de implementación presentado en la tabla 4.1, considerando las implicaciones que estas tienen para la Institución.

a) Costo de implementación

El costo total de la implementación depende del tamaño de la Fundación, grado crítico de la información, tecnología, disposiciones legales y el nivel de protección que se necesita. Por lo que habiendo analizado el resultado de la evaluación de riesgo, se tendrán en cuenta los costos que se muestran en la tabla 4.3.

Tabla 4.3 Detalle de Costos de Implementación de Sistema para FUSALMO

Tipo de Costo	Descripción	Monto
Publicación y capacitación	Comprende gastos de papelería, contratación de medios de divulgación, publicaciones, pago a entidad capacitadora, etc.	$4,500.00
Asistencia externa	Incluye contratación de asesoría externa para elaborar diagnostico general, revisión y actualización de registros existentes, elaboración e implementación de documentos y registros nuevos, realización de auditorías internas y elaboración de avances en periodos establecidos.	$8,000.00
Inversión en tecnología	Se consideran como proyectos de mejora a realizarse post certificación, a menos que represente un obstáculo para la implementación y certificación inicial del sistema. Deberá considerarse como un costo independiente	N/A
Horas hombre	Considerado como gasto administrativo incluido	N/A
Certificación ISO	La contratación de empresa certificadora externa e incluye: Pre auditoria, Auditoria de certificación y emisión del certificado.	$7,500.00
	TOTAL	**$20,000.00**

Fuente: Investigación propia a partir de información relacionada con procesos similares de certificación.

b) Periodo de ejecución:

Este periodo se estima de 12 meses y comprende desde la presentación del proyecto a la dirección ejecutiva y gerencias hasta la obtención de la certificación.

c) Acciones inmediatas:

Como primera acción la divulgación de los resultados de la investigación a la dirección ejecutiva y gerencias, seguido por el levantamiento inmediato de procedimientos en toda la fundación, principalmente los siguientes:

a) Procedimiento de Control de registros.
b) Procedimiento de control de cambios
c) Procedimiento de Gestión de accesos

d) Beneficios a FUSALMO:

Habiendo desarrollado las etapas de diagnóstico antes descritas, los beneficios tangibles e intangibles que percibe la Fundación mediante la implementación de este SGSI son las siguientes:

a) Identificación de riesgos de seguridad y su impacto en la organización.
b) Garantizar el cumplimiento de las características de disponibilidad, confidencialidad e integridad de información.
c) Hacer del conocimiento de la alta dirección de FUSALMO la situación actual en relación a la seguridad de la información.
d) Disponer de los lineamientos para la gestión de incidentes de seguridad.
e) Establecimiento de un comité de seguridad de la información que sea un ente que vigila las buenas prácticas en relación a la seguridad del personal.
f) Fomentar una cultura de seguridad de la información en todos los niveles organizacionales de la Fundación.
g) Capacitar al personal en el tema de seguridad de la información.
h) Adecuada organización de los procesos a través del levantamiento de procedimientos y mejora en la capacidad de reacción.
i) Retroalimentación de la eficiencia del sistema mediante los procesos de auditoria.
j) Minimización de costos en incidentes de seguridad
k) Imagen institucional ante sus aliados estratégicos.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones

a) Mediante el desarrollo de una propuesta de SGSI para FUSALMO, ha sido posible el desarrollo de una metodología de análisis cualitativo y cuantitativo para la identificación de fortalezas, debilidades y riesgos para cualquier organización interesada en implementar este modelo. Proceso que permite focalizar los esfuerzos de mejora y la prevención de incidentes de seguridad.

b) La metodología desarrollada es perfectamente replicable en cualquier otra institución ajena a FUSALMO, ya que parte de las prácticas de seguridad de la información de la organización en relación a un estándar de referencia.

c) A partir de esta experiencia, se ha demostrado que el estándar ISO/IEC 27001:2005 es un referente aplicable para todo tipo de organización interesada en implementar un SGSI; independientemente de su naturaleza, tamaño o giro de negocio; para el caso de FUSALMO siendo una organización dedicada al ámbito educativo, no se encontraron obstáculos para la aplicación del modelo y el análisis desarrollado.

d) Los resultados de la investigación representan un aporte significativo para la Fundación, ya que pretende resolver serias debilidades en la gestión de la seguridad de la información; siendo al mismo tiempo un proceso innovador en nuestro medio, ya que es un estándar en proceso de adopción que aún no es explotado en el sector.

e) La definición del Manual de Políticas de Seguridad es la evidencia o resultado de todo un análisis, traducido en acciones concretas y directrices para la Fundación, que permitirán la administración del Sistema de Gestión de Seguridad de la Información.

f) Se ha establecido un plan de implementación el cual permitirá planificar, organizar y dirigir, cada una de las etapas establecidas para el desarrollo del modelo; permitiendo al mismo tiempo realizar una retroalimentación de la eficiencia de las acciones ejecutadas y la mejora del sistema.

g) El análisis de riesgos es una de las etapas de mayor relevancia en el estudio, ya que permite un mapeo de las amenazas, vulnerabilidades, impacto e identificación de riesgos y su valoración; de modo que, independientemente de la metodología aplicada, es una etapa crítica que debe desarrollarse con tal importancia.

h) Dado que FUSALMO no cuenta con una metodología para análisis económico de incidentes de seguridad de la información, se aplica una metodología basado en los antecedentes de un incidente de seguridad, cuyo resultado refleja costos directos por un monto estimado de $ 2,400, en concepto de pérdidas. Sin embargo, adicionalmente a este monto existen otros costos no cuantificables de carácter crítico, vinculados a proyectos y objetivos de la Fundación que pueden verse comprometidos y representar mayores pérdidas.

5.2 Recomendaciones

a) Promover una cultura de seguridad de la información en la Institución que contemple integralmente la coordinación de las funciones de seguridad, aspectos de confidencialidad, riesgos relacionados a terceros y sistema de auditoría.

b) Se recomienda el levantamiento inmediato de los 11 procedimientos indicados en el apartado 3.8, especialmente los relacionados con el área de Tecnología e Innovación, con el propósito de documentar los procesos objeto de auditoría y protección de la información. Estos procedimientos deben ser impulsados desde la alta dirección y la Gerencia de Tecnología e Innovación.

c) Implementar un plan de auditoría informática que permita registrar y monitorear las operaciones en los sistemas, seguimiento y control de vulnerabilidades e incidentes y evidenciar las debilidades en los procedimientos para su mejora continua.

d) Establecer un Comité de Seguridad de la Información independiente a las áreas de gestión de tecnología de la información, con el propósito de ser un ente imparcial de vigilancia sin conflicto de intereses con la Institución y acorde a los requerimientos del estándar.

e) Ejecutar un plan de formación para la sensibilización del Recurso Humano en relación al tema de seguridad de la información y las implicaciones en los objetivos de la Institución.

f) Divulgar el Manual de Políticas de Seguridad de la Información en todos los niveles jerárquicos, así como la asignación de responsabilidades en las garantías de seguridad en los procesos.

g) Monitorear continuamente los resultados de gestión de la seguridad, a fin de realizar mejoras a los procedimientos y la actualización o incorporación de nuevos procedimientos ante los cambios en la Institución.

h) Realizar evaluaciones de riesgos programadas, a fin de actualizar el diagnóstico de riesgos y el desarrollo de acciones para su prevención o mitigación.

i) Implementar medidas de clasificación de la información con múltiple propósito, no solo seguridad de la información sino también para los propósitos administrativos de back up y segregación.

j) Implementar medidas físicas de restricción a los espacios clave para procesamiento de la información y protección de activos.

k) Establecer e implementar los planes de continuidad del negocio para las áreas críticas de la Fundación, estableciendo responsabilidades, confidencialidad y procedimientos a desarrollar en caso de incidentes o desastres.

l) Definir los requerimientos de seguridad en el comercio electrónico para su planificación.

m) Implementar un registro completo de las actividades en los sistemas y registro de fallas para su análisis y toma de decisiones.

n) Implementar la política de acceso a aplicaciones e información con el fin de brindar respaldo y garantías al proceso de monitoreo, seguimiento y auditoría informática, así como en la gestión de incidentes de seguridad.

o) Implementar la política de confidencialidad enfocada a la responsabilidad de la seguridad y seguimiento de procedimientos, así como la acción disciplinaria que la Institución estime conveniente.

p) Definir el marco regulatorio que regirá los estándares de operación de la Institución ante la ausencia de un ente oficial regulador en el ámbito informático. Esta deberá ser una decisión institucional acorde a sus necesidades.

q) Rediseñar los espacios destinados a procesamiento de información crítica considerando aspectos arquitectónicos de seguridad física y vulnerabilidad ante desastres naturales, condiciones de suministro eléctrico, suministros de red, climatización, sistema contra incendio entre otros.

r) Se recomienda adoptar las siguientes leyes nacionales y estándares a fin de implementar su propio sistema regulatorio: Ley de acceso a la información pública, Ley de equidad de género y estándar ISO 18001 OHSAS Seguridad Laboral.

BIBLIOGRAFÍA

[1] Organización Internacional para la Estandarización. *ISO/IEC 17799:2000 Tecnología de la información – Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información*. Año 2000.

[2] Organización Internacional para la Estandarización. *ISO/IEC 27001:2005 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.* Año 2005

[3] Fundación Salvador del Mundo. Informe de resultados 2011 (PPT). El Salvador. 2011.

[4] Instituto Nacional de Tecnologías de la Comunicación (INTECO). *Guía avanzada de gestión de riesgos.* Disponible en: www.inteco.es/file/TnOIvX7kM5r8OY-S8r9Bmg. España. Año 2008.

[5] Instituto de Ingeniería de Software, Universidad Carnegie Mellon. (Software Engineering Institute). *Metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) para análisis de riesgo.* Estados Unidos. Año 2002

GLOSARIO

A

Activo de información

Este tipo de activo representa los datos de la entidad, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para FUSALMO.

Activo Crítico

Bien tangible o intangible que posee valor para una organización o persona natural y que es indispensable para las actividades fundamentales de la organización.

Ámbito

Contexto de trabajo o desarrollo.

Amenaza

Posibles eventos que pueden desencadenar un incidente, produciendo daños materiales o pérdidas inmateriales en los activos y en las operaciones normales del negocio, interrumpiendo en algunos casos los servicios que prestan.

Análisis de riesgo

Uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

B

Back up o copia de seguridad

Copia de respaldo de la información.

Benchmarking

Proceso sistemático y continuo para evaluar productos y/o servicios, así como procesos de trabajo de otras organizaciones que son reconocidas como practicantes de un proceso determinado.

C

Confidencialidad

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

Control

Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

Continuidad de negocio

Capacidad estratégica y táctica de la organización para planificar y responder ante los incidentes e interrupciones del negocio, con el fin de permitir la continuidad de las actividades comerciales en un nivel aceptable previamente definido.

D

Disponibilidad

Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Data Lost Prevention

Herramienta que identifica, supervisa y protege la información confidencial almacenada, en uso o en tránsito dentro de la red, estaciones de trabajo o dispositivos móviles.

E

Estándar de referencia

En este contexto se refiere al Estándar internacional ISO/IEC 27001:2005 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.

Encriptación

Técnica usada para transformar los datos y su contenido mediante la aplicación de un código secreto con el objeto de evitar que sean conocidos por personas no autorizadas durante su transmisión por canales de comunicaciones o en su almacenamiento en soportes de acceso público.

F

Firewall

Sistema de defensa basado en que el tráfico de entrada o salida a la red pasa por un sistema de seguridad que autoriza, deniega y registra todo evento en función de una política de seguridad; controlando la comunicación interna y externa de la red.

G

Gestión del riesgo.

Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

I

Incidente de seguridad de la información.

Se considera un Incidente de Seguridad de la Información a cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Información

Conjunto organizado de datos procesados, que tienen valor para la organización.

Integridad

Propiedad de salvaguardar la exactitud y estado completo de los activos.

O

Objetivo del estándar

Meta en función de condiciones a lograr.

P

Plan de implementación

Conjunto de actividades a desarrollar en la adopción de un modelo o estrategia.

Perímetro de seguridad

Delimitación de un espacio físico por medio de una barrera (pared, puerta de acceso controlado, entre otros.)

R

Riesgo

Posibilidad de que se produzca un acontecimiento que conlleve a pérdidas materiales en el resultado de las operaciones y actividades que desarrollen las organizaciones.

S

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información; además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no – repudio y confiabilidad.

Sistema de Gestión de Seguridad de la Información

Sistema basado en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

V

Valoración estándar

Puntaje asignado en una escala de valoración definida, como parámetro de comparación de una variable.

ANEXO 1: ESTÁNDAR INTERNACIONAL ISO/IEC 27001:2005 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

ANEXO 2: MODELO DE ENTREVISTA A PERSONAL CLAVE

a) Modelo de entrevista dirigida a la Dirección Ejecutiva

Nombre del puesto de trabajo:	Director Ejecutivo	Fecha:	
Nombre del empleado:			
Guía de entrevista:			
a) ¿Existe una política de seguridad de la información en FUSALMO? b) ¿Quiénes aprueban esta política y cuál es su proceso? c) ¿Cómo es el proceso de divulgación de la política de seguridad de la información a los empleados de la fundación? ¿Esta publicada en manuales u otro medio? d) ¿En la fundación hay un responsable que gestiona la política de seguridad de la información, su desarrollo, revisión y evaluación? e) ¿Se revisa periódicamente esta Política de Seguridad de la Información y como se realiza este proceso? ¿Es planificado? ¿Cómo es aprobado? f) ¿En la revisión de la política de seguridad de la información se incluye la revisión de procedimientos y requisitos?			
g) ¿Cuál es la posición de la Dirección de FUSALMO respecto al apoyo en la implementación de un modelo de gestión de seguridad de la información? h) ¿Qué acciones ha tomado la dirección en función de la Seguridad de la información?			
Documentos relacionados:			

b) Modelo de entrevista dirigida a la Gerencia de Finanzas y Recaudaciones de Fondos

Nombre del puesto de trabajo:	Gerencia de Finanzas y Recaudaciones de Fondos	Fecha:	
Nombre del empleado:			
Guía de entrevista:			
a) ¿Los activos están identificados y se mantiene un inventario o registro actualizado?¿De que manera se realiza? b) ¿Cada activo tiene un propietario identificado, restricciones de acceso definidas y acordadas según una clasificación de seguridad? ¿Estas restricciones son revisadas periódicamente? c) ¿Existen en forma documentada e implementada, regulaciones para el uso adecuado de la información y los activos asociados a una instalación de procesamiento de la información?			
d) ¿En el área que administra se han implementado medidas que garanticen la seguridad de la			

información, estén o no documentadas? ¿Cuáles son? e) ¿Existe alguna clasificación para la información considerando su valor, los requerimientos legales, la sensibilidad y criticidad para la organización? f) ¿Se maneja información confidencial o clasificada, de ser asi como es manejada la seguridad de la información? g) ¿Existe algún mecanismo que garantice que los empleados que tienen acceso a la información clasificada cumplan con las políticas de seguridad implementadas?
h) ¿Anteriormente ha habido incidentes que vulneran la seguridad de la información?¿Como se han manejado estos incidentes?
Documentos relacionados:

c) Modelo de entrevista dirigida a la Gerencia de Recursos Humanos

Nombre del puesto de trabajo:	Gerencia de Recursos Humanos	Fecha:	
Nombre del empleado:			
Guía de entrevista:			
a) ¿Previo al empleo, están definidas y documentadas las funciones de seguridad y responsabilidades del empleado, contratistas y terceros, de conformidad con la política de la organización de seguridad de la información? b) ¿Las funciones y responsabilidades definidas se comunican claramente a los candidatos durante el proceso de previo al empleo? c) Existen reglamentos o procedimientos que rigen la verificación de antecedentes de los candidatos a empleo? d) ¿Los controles de verificación de antecedentes para todos los candidatos a empleo, contratistas y terceros se llevan a cabo de acuerdo con los reglamentos o procedimientos establecidos? e) ¿Los empleados, contratistas y terceros deben firmar un acuerdo de confidencialidad o no divulgación como parte de sus términos y condiciones iniciales del contrato de trabajo? ¿Qué contempla este acuerdo?			
f) ¿Cómo garantizan que los empleados, contratistas y usuarios de terceros apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización? g) ¿Los empleados de la organización, contratistas y usuarios de terceros, reciben formación adecuada acerca de la seguridad y las actualizaciones periódicas de las políticas y procedimientos de la organización en lo que respecta a su función de trabajo? h) ¿Existe un proceso disciplinario formal para los empleados que han cometido una infracción de seguridad? ¿Quién lo hace cumplir y se involucran?			
i) ¿Está definida la responsabilidad para llevar a cabo la terminación del empleo, o cambio de empleo? ¿Cuál es el procedimiento?			

j) ¿Al finalizar el empleo o contrato, existe un proceso que asegura que todos los empleados, contratistas y usuarios de terceras partes renuncian a todos los activos de la organización en su poder, incluyendo información? k) ¿Al terminar el contrato, se eliminan los derechos de acceso de todos los empleados, contratistas y usuarios de terceros, a las instalaciones de procesamiento de la información y la información? ¿Cómo es el procedimiento?
Documentos relacionados:

d) Modelo de entrevista dirigida a la Gerencia de Tecnología e Innovación.

Nombre del puesto de trabajo:	Gerencia de Tecnología e Innovación	Fecha:	
Nombre del empleado:			
Guía de entrevista:			
a) ¿Existe una política de seguridad de la información en FUSALMO? b) ¿Quiénes aprueban esta política y cuál es su proceso? c) ¿Cómo es el proceso de divulgación de la política de seguridad de la información a los empleados de la fundación? ¿Esta publicada en manuales u otro medio? d) ¿En la fundación hay un responsable que gestiona la política de seguridad de la información, su desarrollo, revisión y evaluación? e) ¿Se revisa periódicamente esta Política de Seguridad de la Información y como se realiza este proceso? ¿Es planificado? ¿Cómo es aprobado? f) ¿En la revisión de la política de seguridad de la información se incluye la revisión de procedimientos y requisitos?			
g) ¿Las actividades de seguridad de la información son coordinadas por representantes de las diferentes áreas involucradas: RRHH, mantenimiento, recursos tecnológicos, según sus roles y responsabilidades pertinentes? h) ¿Cómo se define la responsabilidad de seguridad para la protección de activos en procesos específicos, especialmente aquellos que se relacionan con la seguridad de la información? i) ¿Existe un procedimiento para la autorización de nuevos medios de procesamiento de información: software, hardware, entre otros? j) ¿Se han definido los requerimientos de los acuerdos de confidencialidad o no divulgación para la protección de la información? k) ¿Estos acuerdos de confidencialidad son revisados periódicamente? l) ¿Existe un procedimiento que defina la forma en que los incidentes deben ser reportados y además quién y cuándo podrá contactar a las autoridades que den respuesta a estos incidentes, tales como: autoridad judicial, departamento de bomberos, denuncias de abuso, entre otros? m) ¿FUSALMO mantiene contacto con grupos de interés o foros de seguridad especializados y			

asociaciones profesionales en relación a la seguridad de la información?

n) ¿La revisión de políticas, objetivos, controles, procesos y procedimientos, es decir el enfoque de la organización para la seguridad de la información y su implementación, se revisa de forma independiente a intervalos planificados?

o) ¿Previo a otorgar el acceso a terceros, se identifican e implementan las medidas adecuadas, en función de los riesgos para la seguridad de la información y las instalaciones de procesamiento de la información, que implica el acceso de un tercero? ¿Cómo se identifican estos riesgos?

p) ¿Previo a otorgar a los clientes acceso a la información de la organización o de los activos, se cumplen todos los requisitos de seguridad identificados previamente?

q) ¿En los acuerdos con terceros, se cumplen los requisitos de seguridad en cuanto a: la participación de acceso, procesamiento, comunicación y gestión de la información de la organización, instalaciones de procesamiento de la información, o la introducción de productos o servicios para la facilidad del procesamiento de la información?

r) ¿Los empleados, contratistas y terceros deben firmar un acuerdo de confidencialidad o no divulgación como parte de sus términos y condiciones iniciales del contrato de trabajo? ¿Qué contempla este acuerdo?

s) ¿Cómo garantizan que los empleados, contratistas y usuarios de terceros apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización?

t) ¿Los empleados de la organización, contratistas y usuarios de terceros, reciben formación adecuada acerca de la seguridad y las actualizaciones periódicas de las políticas y procedimientos de la organización en lo que respecta a su función de trabajo?

u) ¿Existe un proceso disciplinario formal para los empleados que han cometido una infracción de seguridad? ¿Quién lo hace cumplir y se involucran?

v) ¿Está definida la responsabilidad para llevar a cabo la terminación del empleo, o cambio de empleo? ¿Cuál es el procedimiento?

w) ¿Al finalizar el empleo o contrato, existe un proceso que asegura que todos los empleados, contratistas y usuarios de terceras partes renuncian a todos los activos de la organización en su poder, incluyendo información?

x) ¿Al terminar el contrato, se eliminan los derechos de acceso de todos los empleados, contratistas y usuarios de terceros, a las instalaciones de procesamiento de la información y la información? ¿Cómo es el procedimiento?

y) ¿Cuenta con procedimientos de operación documentados y están disponibles a todos los usuarios cuando sea requerido?

z) ¿Los cambios de los medios y sistemas de procesamiento de la información están controlados?

aa) ¿Se encuentran aisladas las instalaciones de prueba con las instalaciones operacionales de sistemas?

bb) ¿Se tiene asegurado que los terceros implementan, operan y mantienen los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega de los servicios de terceros?

cc) ¿Son auditados regularmente los servicios prestados por terceros?

dd) ¿Son monitoreadas la capacidad, demanda y los requerimientos de las proyecciones futuras,

asegurando que la fuente de procesamiento y almacenamiento se encuentre disponible?

ee) ¿Se tienen establecidos los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas?

ff) ¿Las pruebas realizadas al sistema son ejecutadas antes de la aceptación de este?

gg) ¿Son desarrollados e implementados apropiadamente las alertas de detección, recuperación de la información y prevención, en caso se presente un código malicioso?

hh) ¿La ejecución de código móvil no autorizados son denegados?

ii) ¿Las copias de seguridad de información y software son utilizadas y probadas periódicamente de acuerdo con la política de respaldo establecida?

jj) ¿Toda la información esencial y software se puede recuperar después de un desastre o mal funcionamiento en los medios de almacenamiento?

kk) ¿Existen procedimientos para la administración de dispositivos extraíbles como memorias USB, discos duros externos, tarjetas de memoria?

ll) ¿Existe una política, procedimiento y control en sitio del intercambio de la información que asegure la protección de la información?

mm) ¿La información involucrada en la mensajería electrónica está protegida?

nn) ¿La información involucrada en el comercio electrónico pasando sobre la red pública está protegida de la actividad fraudulenta, disputa de contrato, y cualquier acceso no autorizado o modificación?

oo) ¿La información involucrada en las transacciones en línea está protegida para prevenir la trasmisión incompleta, mal enrutamiento, alteración de mensaje no autorizado y la reproducción o duplicación no autorizada?

pp) ¿ Se mantienen registros de las actividades de auditoria, excepciones y eventos de seguridad de la información, estos son mantenidos por un periodo de tiempo acordado para ayudar en investigaciones futuras y monitoreo del control de acceso?

qq) ¿Existe una política de control de acceso desarrollada y revisada en base a los requerimientos comerciales y de seguridad?

rr) ¿A los usuarios y proveedores de servicios se les dio una declaración clara de los requerimientos operativos que deben cumplir ante los controles de acceso?

ss) ¿La asignación y uso de privilegios en el entorno del sistema de información está restringido y controlado?

tt) ¿La asignación y reasignación de las contraseñas están controlados a través de un proceso formal de gestión?

uu) ¿A los usuarios se les pide que firmen una declaración para mantener la confidencialidad de la contraseña?

vv) ¿Hay alguna práctica de seguridad para guiar a los usuarios en la selección y el mantenimiento de contraseñas seguras?

ww) ¿La organización ha adoptado la política de escritorio limpio en lo que respecta a los documentos y medios de almacenamiento extraíbles y la política de pantalla limpia en lo que respecta a los medios de procesamiento de la información?

xx) ¿Existen controles del ruteo de las redes para asegurar que las conexiones de cómputo y flujos de información no infrinjan las políticas de control de acceso de las aplicaciones comerciales?

yy) ¿El acceso al sistema operativo está controlado por procedimientos de seguridad en el inicio de sesión?

zz) ¿A todos los usuarios se les proporciona una identificación única (ID de usuario) para su uso personal y exclusivo, incluye a operadores, administradores de sistemas y todo el resto del personal, incluyendo técnicos?

aaa) ¿Las sesiones inactivas se cierran después de un período definido de inactividad?

bbb) ¿Los sistemas vulnerables o sensibles poseen un ambiente aislado?

ccc) ¿El acceso a la información y funciones de aplicación del sistema está restringido para los usuarios y personal de apoyo, de acuerdo con la política de control de acceso definidas?

ddd) ¿Los requisitos de seguridad para los nuevos sistemas de información y la mejora de los sistemas de información existentes, especifican los requisitos para los controles de seguridad?

eee) ¿La organización tiene una política sobre el uso de controles criptográficos para la protección de la información y es aplicada con éxito?

fff) ¿Se ha implementado procedimientos para controlar la instalación de software en los sistemas operativos?

ggg) ¿Se ha implementado estrictos controles para restringir el acceso al código fuente de los programas?

hhh) ¿Se ha implementado un proceso o procedimiento para revisar y comprobar las aplicaciones críticas de negocio ante un impacto adverso en las operaciones de la organización o de la seguridad después de los cambios al sistema operativo?

iii) ¿Se genera información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan?¿La organización presenta las vulnerabilidades evaluadas y las medidas adecuadas que han sido adoptadas para mitigar el riesgo asociado?

jjj) ¿Se ha establecido responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información?

kkk) ¿Se ha implementado un mecanismo para identificar y cuantificar el tipo, volumen y costos de los incidentes de seguridad de la información?

lll) ¿La información obtenida de la evaluación de los últimos incidentes de seguridad de la información se utiliza para identificar los incidentes recurrentes o de alto impacto?

mmm) ¿Las evidencias relacionadas con el incidente son recolectadas, retenidas y presentadas conforme a las normas de manejo de evidencia?

nnn) ¿Existe un proceso controlado de los requisitos de seguridad de la información para desarrollar y mantener la continuidad del negocio en toda la organización?

ooo) ¿Se desarrollan planes para mantener y restaurar las operaciones de negocio, asegurar la disponibilidad de la información en el nivel requerido y en el marco de tiempo requerido después de una interrupción o falla de los procesos del negocio?

ppp) ¿El plan de continuidad del negocio asegura que todos los miembros del equipo de recuperación y personal pertinente están al tanto de los planes, su responsabilidad para la continuidad del negocio y seguridad de la información, y conocen su función cuando el plan lo indica?

qqq) ¿Se han definido de forma explícita y documentada para cada sistema de información y organización, todos los requisitos legales pertinentes, los reguladores, contractuales y el enfoque de la organización para cumplir con los requisitos?

rrr) ¿Los registros importantes de la organización estan protegidos ante la destrucción, pérdida y falsificación, de acuerdo con el requisito legal, reglamentario, contractual y los requerimientos del negocio?

Documentos relacionados:

e) Modelo de entrevista dirigida a la Coordinación de Recursos Tecnológicos.

Nombre del puesto de trabajo:	Coordinación de recursos tecnológicos	Fecha:	
Nombre del empleado:			
Guía de entrevista:			
a) ¿Las actividades de seguridad de la información son coordinadas por representantes de las diferentes áreas involucradas: RRHH, mantenimiento, recursos tecnológicos, según sus roles y responsabilidades pertinentes? b) ¿Cómo se define la responsabilidad de seguridad para la protección de activos en procesos específicos, especialmente aquellos que se relacionan con la seguridad de la información? c) ¿Existe un procedimiento para la autorización de nuevos medios de procesamiento de información: software, hardware, entre otros? d) ¿Se han definido los requerimientos de los acuerdos de confidencialidad o no divulgación para la protección de la información? e) ¿Estos acuerdos de confidencialidad son revisados periódicamente? f) ¿Existe un procedimiento que defina la forma en que los incidentes deben ser reportados y además quién y cuándo podrá contactar a las autoridades que den respuesta a estos incidentes, tales como: autoridad judicial, departamento de bomberos, denuncias de abuso, entre otros? g) ¿FUSALMO mantiene contacto con grupos de interés o foros de seguridad especializados y asociaciones profesionales en relación a la seguridad de la información? h) ¿La revisión de políticas, objetivos, controles, procesos y procedimientos, es decir el enfoque de la organización para la seguridad de la información y su implementación, se revisa de forma independiente a intervalos planificados?			
i) ¿Previo a otorgar el acceso a terceros, se identifican e implementan las medidas adecuadas, en función de los riesgos para la seguridad de la información y las instalaciones de procesamiento de la información, que implica el acceso de un tercero? ¿Cómo se identifican estos riesgos? j) ¿Previo a otorgar a los clientes acceso a la información de la organización o de los activos, se cumplen todos los requisitos de seguridad identificados previamente? k) ¿En los acuerdos con terceros, se cumplen los requisitos de seguridad en cuanto a: la participación de acceso, procesamiento, comunicación y gestión de la información de la organización, instalaciones de procesamiento de la información, o la introducción de productos o servicios para la facilidad del procesamiento de la información?			
l) ¿Los activos están identificados y se mantiene un inventario o registro actualizado? m) ¿Cada activo tiene un propietario identificado, restricciones de acceso definidas y acordadas según una clasificación de seguridad? ¿Estas restricciones son revisadas periódicamente? n) ¿Existen en forma documentada e implementada, regulaciones para el uso adecuado de la información y los activos asociados a una instalación de procesamiento de la información?			
o) ¿Existe alguna clasificación para la información considerando su valor, los requerimientos legales, la sensibilidad y criticidad para la organización?			

p) ¿Existe un procedimiento definido para el etiquetado de información y la manipulación, de acuerdo con el esquema de clasificación adoptado por la organización?
q) ¿Cómo garantizan que los empleados, contratistas y usuarios de terceros apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización? r) ¿Los empleados de la organización, contratistas y usuarios de terceros, reciben formación adecuada acerca de la seguridad y las actualizaciones periódicas de las políticas y procedimientos de la organización en lo que respecta a su función de trabajo? s) ¿Existe un proceso disciplinario formal para los empleados que han cometido una infracción de seguridad? ¿Quién lo hace cumplir y se involucran?
t) ¿Está definida la responsabilidad para llevar a cabo la terminación del empleo, o cambio de empleo? ¿Cuál es el procedimiento? u) ¿Al finalizar el empleo o contrato, existe un proceso que asegura que todos los empleados, contratistas y usuarios de terceras partes renuncian a todos los activos de la organización en su poder, incluyendo información? v) ¿Al terminar el contrato, se eliminan los derechos de acceso de todos los empleados, contratistas y usuarios de terceros, a las instalaciones de procesamiento de la información y la información? ¿Cómo es el procedimiento?
w) ¿Cuenta con procedimientos de operación documentados y están disponibles a todos los usuarios cuando sea requerido? x) ¿Los cambios de los medios y sistemas de procesamiento de la información están controlados? y) ¿Se encuentran aisladas las instalaciones de prueba con las instalaciones operacionales de sistemas? z) ¿Se tiene asegurado que los terceros implementan, operan y mantienen los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega de los servicios de terceros? aa) ¿Son auditados regularmente los servicios prestados por terceros? bb) ¿Son monitoreadas la capacidad, demanda y los requerimientos de las proyecciones futuras, asegurando que la fuente de procesamiento y almacenamiento se encuentre disponible? cc) ¿Se tienen establecidos los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas? dd) ¿Las pruebas realizadas al sistema son ejecutadas antes de la aceptación de este? ee) ¿Son desarrollados e implementados apropiadamente las alertas de detección, recuperación de la información y prevención, en caso se presente un código malicioso? ff) ¿La ejecución de código móvil no autorizados son denegados? gg) ¿Las copias de seguridad de información y software son utilizadas y probadas periódicamente de acuerdo con la política de respaldo establecida? hh) ¿Toda la información esencial y software se puede recuperar después de un desastre o mal funcionamiento en los medios de almacenamiento? ii) ¿Existen procedimientos para la administración de dispositivos extraíbles como memorias USB, discos duros externos, tarjetas de memoria? jj) ¿Existe una política, procedimiento y control en sitio del intercambio de la información que asegure la protección de la información? kk) ¿La información involucrada en la mensajería electrónica está protegida? ll) ¿La información involucrada en el comercio electrónico pasando sobre la red pública está protegida de la actividad fraudulenta, disputa de contrato, y cualquier acceso no autorizado o

modificación?

mm) ¿La información involucrada en las transacciones en línea está protegida para prevenir la trasmisión incompleta, mal enrutamiento, alteración de mensaje no autorizado y la reproducción o duplicación no autorizada?

nn) ¿ Se mantienen registros de las actividades de auditoria, excepciones y eventos de seguridad de la información, estos son mantenidos por un periodo de tiempo acordado para ayudar en investigaciones futuras y monitoreo del control de acceso?

oo) ¿Existe una política de control de acceso desarrollada y revisada en base a los requerimientos comerciales y de seguridad?

pp) ¿A los usuarios y proveedores de servicios se les dio una declaración clara de los requerimientos operativos que deben cumplir ante los controles de acceso?

qq) ¿La asignación y uso de privilegios en el entorno del sistema de información está restringido y controlado?

rr) ¿La asignación y reasignación de las contraseñas están controlados a través de un proceso formal de gestión?

ss) ¿A los usuarios se les pide que firmen una declaración para mantener la confidencialidad de la contraseña?

tt) ¿Hay alguna práctica de seguridad para guiar a los usuarios en la selección y el mantenimiento de contraseñas seguras?

uu) ¿La organización ha adoptado la política de escritorio limpio en lo que respecta a los documentos y medios de almacenamiento extraíbles y la política de pantalla limpia en lo que respecta a los medios de procesamiento de la información?

vv) ¿Existen controles del ruteo de las redes para asegurar que las conexiones de cómputo y flujos de información no infrinjan las políticas de control de acceso de las aplicaciones comerciales?

ww) ¿El acceso al sistema operativo está controlado por procedimientos de seguridad en el inicio de sesión?

xx) ¿A todos los usuarios se les proporciona una identificación única (ID de usuario) para su uso personal y exclusivo, incluye a operadores, administradores de sistemas y todo el resto del personal, incluyendo técnicos?

yy) ¿Las sesiones inactivas se cierran después de un período definido de inactividad?

zz) ¿Los sistemas vulnerables o sensibles poseen un ambiente aislado?

aaa) ¿El acceso a la información y funciones de aplicación del sistema está restringido para los usuarios y personal de apoyo, de acuerdo con la política de control de acceso definidas?

bbb) ¿Los requisitos de seguridad para los nuevos sistemas de información y la mejora de los sistemas de información existentes, especifican los requisitos para los controles de seguridad?

ccc) ¿La organización tiene una política sobre el uso de controles criptográficos para la protección de la información y es aplicada con éxito?

ddd) ¿Se ha implementado procedimientos para controlar la instalación de software en los sistemas operativos?

eee) ¿Se ha implementado estrictos controles para restringir el acceso al código fuente de los programas?

fff) ¿Se ha implementado un proceso o procedimiento para revisar y comprobar las aplicaciones críticas de negocio ante un impacto adverso en las operaciones de la organización o de la seguridad después de los cambios al sistema operativo?

ggg) ¿Se genera información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan?¿La organización presenta las vulnerabilidades evaluadas y las

medidas adecuadas que han sido adoptadas para mitigar el riesgo asociado?

hhh) ¿Se ha establecido responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información?

iii) ¿Se ha implementado un mecanismo para identificar y cuantificar el tipo, volumen y costos de los incidentes de seguridad de la información?

jjj) ¿La información obtenida de la evaluación de los últimos incidentes de seguridad de la información se utiliza para identificar los incidentes recurrentes o de alto impacto?

kkk) ¿Las evidencias relacionadas con el incidente son recolectadas, retenidas y presentadas conforme a las normas de manejo de evidencia?

lll) ¿Existe un proceso controlado de los requisitos de seguridad de la información para desarrollar y mantener la continuidad del negocio en toda la organización?

mmm) ¿Se desarrollan planes para mantener y restaurar las operaciones de negocio, asegurar la disponibilidad de la información en el nivel requerido y en el marco de tiempo requerido después de una interrupción o falla de los procesos del negocio?

nnn) ¿El plan de continuidad del negocio asegura que todos los miembros del equipo de recuperación y personal pertinente están al tanto de los planes, su responsabilidad para la continuidad del negocio y seguridad de la información, y conocen su función cuando el plan lo indica?

ooo) ¿Se han definido de forma explícita y documentada para cada sistema de información y organización, todos los requisitos legales pertinentes, los reguladores, contractuales y el enfoque de la organización para cumplir con los requisitos?

ppp) ¿Los registros importantes de la organización estan protegidos ante la destrucción, pérdida y falsificación, de acuerdo con el requisito legal, reglamentario, contractual y los requerimientos del negocio?

qqq) ¿Se ha establecido perímetros de seguridad física para proteger las áreas de procesamiento de la información, tales como vigilancia, barreras físicas, sistemas de alarma, entre otros?

rrr) ¿Los controles de entrada están instalados de modo que solo el personal autorizado de determinadas áreas de la organización tiene acceso?

sss) ¿Las instalaciones donde se procesa el servicio de la información están resguardados y protegidos?

ttt) ¿Cuentan sistema contra incendios, medidas de seguridad ante inundaciones, terremotos y otros fenómenos naturales o producidos por el hombre?

uuu) ¿Están controladas las áreas de acceso o puntos donde personas no-autorizadas puedan ingresar a las instalaciones.

vvv) ¿Los equipos están protegidos contra amenazas, peligros ambientales y accesos no autorizados?

www) ¿El equipo está protegido contra fallas de energía y otras interrupciones?

xxx) ¿La fuente de alimentación y el cable de telecomunicaciones que transporta datos está protegido contra interrupciones o daños?

yyy) ¿Existe algún control adicional en sitio para proteger la información sensible o crítica?

zzz) ¿Los equipos tienen su mantenimiento apropiado para asegurar la disponibilidad y la integridad?

aaaa) ¿Los equipos cuentan con el mantenimiento recomendado por el proveedor de servicios y en los intervalos de tiempo recomendables?

bbbb) ¿El mantenimiento de los equipos es desarrollado solo por personal autorizado?

cccc) ¿Si los equipos son enviados fuera de las instalaciones, cuentan con los controles

apropiados? dddd) ¿Son evaluados los riesgos al usar los equipos fuera de las de las instalaciones de la organización y se han implementados controles de mitigación? eeee) ¿El procesamiento de la información fuera de las instalaciones de la organización son autorizados por la dirección? ffff) ¿Los equipos que contienen medios de almacenamiento son chequeados para asegurar que se les haya removido o sobre-escrito de manera segura cualquier dato confidencial y software con licencia, antes de su eliminación?
Documentos relacionados:

f) Modelo de entrevista dirigida a la Coordinación de Mantenimiento.

Nombre del puesto de trabajo:	Coordinación de mantenimiento	Fecha:	
Nombre del empleado:			
Guía de entrevista:			
a) ¿Se ha establecido perímetros de seguridad física para proteger las áreas de procesamiento de la información, tales como vigilancia, barreras físicas, sistemas de alarma, entre otros? b) ¿Los controles de entrada están instalados de modo que solo el personal autorizado de determinadas áreas de la organización tiene acceso? c) ¿Las instalaciones donde se procesa el servicio de la información están resguardados y protegidos? d) ¿Cuentan sistema contra incendios, medidas de seguridad ante inundaciones, terremotos y otros fenómenos naturales o producidos por el hombre? e) ¿Están controladas las áreas de acceso o puntos donde personas no-autorizadas puedan ingresar a las instalaciones.			
f) ¿Los equipos están protegidos contra amenazas, peligros ambientales y accesos no autorizados? g) ¿El equipo está protegido contra fallas de energía y otras interrupciones? h) ¿La fuente de alimentación y el cable de telecomunicaciones que transporta datos está protegido contra interrupciones o daños? i) ¿Los equipos tienen su mantenimiento apropiado para asegurar la disponibilidad y la integridad? j) ¿Los equipos cuentan con el mantenimiento recomendado por el proveedor de servicios y en los intervalos de tiempo recomendables? k) ¿El mantenimiento de los equipos es desarrollado solo por personal autorizado? l) ¿Si los equipos son enviados fuera de las instalaciones, cuentan con los controles apropiados? m) ¿Son evaluados los riesgos al usar los equipos fuera de las de las instalaciones de la organización y se han implementados controles de mitigación?			
Documentos relacionados:			

MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION

FUNDACIÓN SALVADOR DEL MUNDO (FUSALMO)

OCTUBRE DE 2012, SOYAPANGO.

EL SALVADOR, CENTRO AMÉRICA

1. INTRODUCCIÓN

La Fundación, reconoce la información como un activo fundamental en las operaciones y el logro de objetivos definidos por la estrategia de la institución, razón por la cual establece un marco en el cual se asegure que la información está protegida y disponible independientemente de la forma en la que se maneje, procese, transporte y almacene.
Por tanto, este documento describe los lineamientos y políticas de seguridad de la información y la forma en que deberá administrarse la gestión para su cumplimiento**.** Para la elaboración del mismo, se toman como base las leyes y regulaciones aplicables, especificados en este caso en el estándar ISO/IEC 27001:2005.
Las políticas descritas en este manual forman parte esencial del **Sistema de Gestión de Seguridad de la Información** y son la referencia para la implementación de los controles, procedimientos y estándares específicos.
Para la Institución, lo estipulado en este Manual de Seguridad de la Información, tiene prioridad y un compromiso de responsabilidad de todos los miembros de la fundación para velar y garantizar que todas las prácticas deben ir en coherencia con el sentido y espíritu de las mismas.

2. OBJETIVO

El objetivo de este Sistema de Gestión de Seguridad de la Información es propiciar y asegurar condiciones razonables que permitan proteger los activos de información en su integridad, confidencialidad y disponibilidad en la Fundación Salvador del Mundo, con el fin de regular la gestión y generar confianza en los clientes internos y externos.

3. ALCANCE

Las políticas de seguridad de la información aquí especificadas, contemplan los aspectos administrativos y de control que deben ser cumplidos por los colaboradores y terceros que laboren o tengan relación con la Fundación Salvador del Mundo, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información.

4. VIGENCIA Y ACTUALIZACIÓN DEL MANUAL, DOCUMENTOS Y REGISTROS

Es responsabilidad del Comité de Seguridad de la Información y Junta Directiva de FUSALMO la definición, actualización y mantenimiento del Manual de Políticas de Seguridad de la Información de la Fundación.

Debiendo tener en cuenta para las respectivas revisiones establecidas en el control de documentos y registros, un periodo de vigencia 4 años para toda la documentación, incluyendo este manual del SGC.
Las actualizaciones de estos documentos antes de la finalización del periodo establecido, podrá ser por causas como:

- Los incidentes de seguridad
- Nuevas vulnerabilidades identificadas
- Cambios organizacionales o tecnológicos, en los procesos, en los objetivos del sistema o de la fundación
- Mejoras a los procesos
- Otros.

5. HOJA DE CONTROL DE REVISIONES

No. REVISION	FECHA REVISION	FECHA INSERTADA	INSERTADA POR

Esta hoja se utiliza para mantener el control de las revisiones del manual. Cuando se reciba una revisión, deberá anotarse toda la información solicitada en este cuadro y se insertarán las nuevas hojas en el manual. La Gerencia de Tecnología e Innovación conservará por un período de seis meses las hojas retiradas después de una revisión. No se permiten enmiendas y revisiones escritas a mano excepto en situaciones en las cuales se necesite hacerlas a beneficio de la seguridad.

6. SOLICITUD DE CAMBIOS EN EL MANUAL

Cualquier usuario asignado a la fundación puede someter una solicitud a través de su jefe para cambiar o modificar información contenida en este manual.

La solicitud de cambio se realizara utilizando el siguiente formato:

Nombre/ Departamento del solicitante: _____

Firma del Jefe del Departamento Aprobando: _____

Firma del Gerente del Departamento Aprobando: _____

Listar el manual, sección, página y párrafo propuesto a ser revisado:

_____

Anotar el cambio solicitado o adjuntarlo a esta página: _____

_____

_____

_____

El Gerente de Tecnología e Innovación, se encargará de evaluar la solicitud y si procede hará la inclusión en la siguiente revisión del manual a ser sometido a la Junta Directiva.

Si la solicitud es rechazada, el Gerente notificará al solicitante. La notificación listará las razones del porque la solicitud fue desaprobada.

Todas las revisiones de este manual serán coordinadas con el Gerente de Tecnología e Innovación antes de ser aprobadas y publicadas a efecto de asegurar que no exista conflicto con otros manuales.

7. REGISTRO DE CAMBIOS RELEVANTES

Los siguientes cambios al Manual de Políticas de Seguridad de la Información han sido desarrollados en su Revisión 00:

Sección	Página	Detalle de los Cambios

8. IDENTIFICACION DE REVISIONES

Cuando una revisión es emitida, una línea a lo largo del margen izquierdo identificará todo el material corregido.

Toda revisión se actualiza en el encabezado de cada página, con su fecha y número de revisión correspondiente, sin afectar el resto del manual.

9. GLOSARIO

Activo de información: Este tipo de activo representa los datos de la entidad, información que tiene valor para los procesos de negocio, independientemente de su ubicación puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para FUSALMO.

Análisis de riesgos: Uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

Backup o copia de seguridad: Copia de respaldo de la información.

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

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

Criticidad: Medida del impacto que tendría la institución debido a una falla de un sistema y que éste no funcione como es requerido.

Custodio: Ente, área, proceso o persona encargada de preservar y resguardar la información entregada y que generalmente son de propiedad de otro proceso o área.

Desastre: Hecho natural o provocado por el ser humano que afecta negativamente a la vida, industria y desemboca con frecuencia en cambios permanentes en las sociedades humanas.

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

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Evento de Seguridad de la Información: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Incidente de Seguridad de la Información: Se considera un Incidente de Seguridad de la Información a cualquier evento que haya vulnerado la seguridad

de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Infraestructura de Procesamiento de Información: Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Medios en tránsito: Son todos aquellos dispositivos autorizados por FUSALMO, que permiten el almacenamiento de información, los cuales pueden ingresar o salir de las instalaciones de la compañía con la respectiva autorización. Se incluyen equipos portátiles, PDAs, Ipods, reproductores mp3, teléfonos celulares, memorias USB/SD/Mini-SD, CDs, DVDs, respaldo y similares. Asimismo se incluyen correos electrónicos y conexiones por donde pueda ser transportada la información de la empresa.

Medio removible: Medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, diskettes, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB.

Propietario/responsable: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

Responsable de activo de información: es un colaborador o área de la Gerencia de Tecnología e Innovación de velar porque la información a su cargo sea protegida de manera adecuada.

Sensibilidad: Nivel de impacto que una divulgación no autorizada podría generar.

Servicio: es cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

Soportes físicos: Datos en soporte papel (cartas, informes, normas, contratos) o en medios de almacenamiento físico.

Terceros: Se entiende por tercero a toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

10. POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Para la Institución, la información representa un activo fundamental para el desarrollo de sus procesos y prestación de servicios, así como un insumo valioso para la toma de decisiones eficientes. Motivo por el cual reconoce un compromiso institucional a nivel de protección de sus activos más significativos como parte de una visión orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.
Establece una herramienta que le permite: identificar y minimizar los riesgos a los cuales se expone la información, reducir los costos operativos y financieros, establecer una cultura de seguridad y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes, canalizados a través de la implementación de un Sistema de Gestión de Seguridad de la Información.
El proceso de análisis y determinación de riesgos de los activos de información representa la base para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados; este proceso será liderado por el Coordinador del Comité de Seguridad de la Información.
Además, se compromete a implementar y mantener en el desarrollo de su Sistema de Gestión de Seguridad de la Información, programas de capacitación en toda la Institución, con el propósito de minimizar la ocurrencia y el impacto de incidentes de seguridad de la información como parte de sus procesos de mejora continua.
Esta política deberá ser revisada y actualizada con regularidad en el marco del proceso de revisión gerencial, o cuando se identifiquen cambios en procesos o actividades; cambio en su estructura, objetivos o alguna condición que afecte la política, para así garantizar que sigue siendo adecuada a los requerimientos especificados.

11. COMPROMISO DE LA DIRECCIÓN

La Junta Directiva es el ente que acepta y aprueba la Política de Seguridad de la Información como parte del compromiso en el diseño e implementación de políticas que garanticen la integridad, confidencialidad y disponibilidad de la información de la Fundación.
La Junta Directiva y la Dirección Ejecutiva demostrarán su apoyo y compromiso mediante lo siguiente:

a) Revisar y aprobar las Políticas de Seguridad de la Información definidas en este documento.

b) Promover una cultura de seguridad.

c) Divulgar este manual a todos los miembros y niveles de la fundación.

d) Brindar apertura y disponibilidad necesaria para asegurar los recursos adecuados para implementar y mantener las Políticas de Seguridad de la Información.

e) Verificar el cumplimiento de las políticas de seguridad de la información que se listan en este manual.

12. REGULACIÓN

Las políticas dictadas en este manual, deberán ser reconocidas, aceptadas y cumplidas por todo colaborador, miembros o terceros que tengan relación directa con la Institución. En caso de incumplimiento de éstas, se considerará como un incidente de seguridad, que de acuerdo al caso podrá dar lugar a un proceso disciplinario y sancionatorio para los colaboradores, miembros o terceros y se convertirá en una causa válida de finalización de contrato con los colaboradores o contratistas

13. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

Las siguientes Políticas de Seguridad de la Información, representan la visión institucional en relación a la protección de los activos de información:

a) Existirá un Comité de Seguridad de la Información, el cual tendrá la responsabilidad de revisar, dar seguimiento y mejora al Sistema de Gestión de Seguridad de la Información.

b) Los activos de información, serán identificados y clasificados con el propósito de establecer los mecanismos de protección necesarios.

c) Se definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados y pérdida de integridad, los cuales deberán garantizar la disponibilidad requerida por los colaboradores, miembros y usuarios de los servicios de la Fundación.

d) Todos los colaboradores, miembros, terceros y/o contratistas serán responsables de garantizar la protección de la información a la cual accedan o procesen, a fin de evitar su pérdida, alteración, destrucción o uso indebido.

e) Se ejecutarán auditorías y controles periódicos para verificar el cumplimiento del Sistema de Gestión de Seguridad de la Información.

f) Exclusivamente se permitirá el uso de software autorizado que haya sido legalmente adquirido por la fundación.

g) Es responsabilidad de los colaboradores, miembros, terceros y contratistas reportar los Incidentes de Seguridad, eventos sospechosos y mal uso de los recursos que identifiquen en sus funciones.

h) Las violaciones y/o adulteraciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

i) La Institución contará con un Plan de Continuidad del Negocio que asegure la continuidad en el desarrollo de las actividades y operaciones ante la ocurrencia de incidentes no previstos, provocados o desastres naturales.

14. ORGANIZACIÓN DE LA FUNCIÓN DE SEGURIDAD DE LA INFORMACIÓN Ref.: ISO/IEC 27001:2005 A.6

14.1 Coordinación de la función de Seguridad de la Información [ISO/IEC 27001:2005 A.6.1.2; A.6.1.3]

La Institución establece un Comité de Seguridad de la Información, conformado por un grupo interdisciplinario de colaboradores, que será responsable del análisis, revisión y centralización de las acciones relacionadas con la gestión de Seguridad de la Información de la Fundación, con el fin de mantener la vigencia de las políticas de acuerdo con las necesidades y requisitos de las operaciones de la Fundación.
Los integrantes del comité deberán tener las siguientes características:

a) Disciplina.
b) Conocimiento de las operaciones de la empresa
c) Confidencialidad
d) Capacidad de trajo en equipo
e) Propositivos.

14.2 Autorización para el Uso de Infraestructura de Información *[ISO/IEC 27001:2005 A.6.1.4]*

La adquisición de infraestructura nueva para el procesamiento de información (equipos, software, aplicaciones e instalaciones físicas) debe ser analizada y revisada por el Comité de Seguridad de la Información y la jefatura del área afectada. Esta autorización será de acuerdo a los procedimientos respectivos y asegurará que las políticas de seguridad sean cumplidas en su totalidad.

14.3 Acuerdos de Confidencialidad
[ISO/IEC 27001:2005 A.6.1.5]

Todos los colaboradores, miembros y terceros deben aceptar los acuerdos de confidencialidad definidos por la Fundación, los cuales deberán expresar los compromisos de buenas prácticas de protección y uso de la información de acuerdo con los criterios establecidos en ella.
Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita a personas o entidades externas el acceso a la información y/o a los recursos de la Institución.
Estos acuerdos deben ser aceptados como parte del proceso de contratación, razón por la cual esta cláusula y/o acuerdo de confidencialidad forma parte integral de cada uno de los contratos y en caso de violación deberán asumir las consecuencias y sanciones respectivas.

14.4 Contacto con las Autoridades y con Grupos de Interés Especiales
[ISO/IEC 27001:2005 A.6.1.6; A.6.1.7]

La Institución debe establecer y mantener contacto cercano con autoridades (Policía Nacional Civil, bomberos, entre otros), así como con grupos de interés o foros de especialistas en seguridad, para poder ser contactados oportunamente en caso de presentarse un incidente de seguridad de la información.

14.5 Auditorías Internas
[ISO/IEC 27001:2005 A.6.1.8]

Se programará y ejecutará revisiones internas a su Sistema de Gestión de Seguridad de la Información con el fin de determinar la conformidad de las políticas, procedimientos y controles establecidos dentro del sistema con lo acordado en este manual, el cual debe estar actualizado de acuerdo a la mejora continua en la Fundación. Para tal propósito se verificarán requerimientos de seguridad, regulaciones aplicables, y si éstos se encuentran implementados y mantenidos eficazmente. Además, debe definir un programa de auditorías y basado en ello éstas deberán ser ejecutadas. En caso de ser necesario se pueden programar revisiones parciales o totales sobre un proceso, área, etc. Ello con el propósito de verificar la eficacia de las acciones correctivas cuando sean identificadas como no conformidades. Las auditorías al Sistema de Gestión de Seguridad de la Información podrán ser desarrolladas por cualquier colaborador, miembro y/o tercero que cumpla con el perfil, los requisitos establecidos por la fundación y mantenga un criterio de revisión objetiva en el cual no audite la misma área involucrada.

14.6 Riesgos Relacionados con Terceros
[ISO/IEC 27001:2005 A.6.2.2]

La Institución determina los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información e infraestructura para su procesamiento por parte de terceros, con el fin de establecer los mecanismos de control necesarios para garantizar la seguridad. Los controles que a partir del análisis de riesgos se establezcan como necesarios, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos de confidencialidad, previamente a la entrega de los accesos requeridos.

15. GESTIÓN DE ACTIVOS DE INFORMACIÓN
Ref.: ISO/IEC 27001:2005 A.7

15.1 Inventario de Activos de Información
[ISO/IEC 27001:2005 A.7.1.1; A.7.1.2]

Los diferentes departamentos, colaboradores, miembros y/o terceros deben garantizar el adecuado uso, administración y control sobre los activos de la fundación, deben mantener un inventario actualizado de los activos que se encuentran dentro del alcance del Sistema de Gestión de Seguridad de la Información. El consolidado actualizado de los activos informáticos quedará en custodia del Comité de Seguridad de la Información.

15.2 Uso Adecuado de los Activos
[ISO/IEC 27001:2005 A.7.1.3]

Son activos propiedad de la Institución: la información, archivos físicos, sistemas, servicios, y equipos (equipos de escritorio, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fax, entre otros), los cuales se proporcionan a los colaboradores, miembros y terceros autorizados, para cumplir con los propósitos de la fundación.
Por tanto, la Fundación podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en este manual y en cualquier proceso legal que se requiera, cuando ésta lo estime conveniente.
Las normas relacionadas con el acceso y las restricciones a los documentos públicos, determinarán las condiciones de acceso a los documentos físicos y digitales.
La consulta o revisión de información contenida en expedientes o documentos que están en custodia de la Institución se permitirá en días y horas laborales, con la presencia del colaborador o jefe inmediato responsable. Estos privilegios serán

establecidos por el Jefe de área, quien comunicará al responsable de administración del software el listado con los colaboradores y sus privilegios.
La importancia y daño o alteración al que estén sujetos los documentos físicos, determinará las restricciones y reserva a los que están sujetos; para lo cual, el Gerente del área será el responsable de determinar el carácter de reserva o restricción de dichos documentos.
Todos los colaboradores, miembros y terceros que manipulen información en el desarrollo de sus funciones deben someterse a lo descrito en el acuerdo de confidencialidad de la información, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos en este manual para la clasificación de la información.

15.3 Acceso a Internet

La Institución debe controlar, verificar y monitorear el uso adecuado de este recurso para todos los casos, bajo los siguientes lineamientos:

a) No está permitido:
   a. El acceso a cualquier página en contra de la ética moral o de procedencia poco segura.
   b. El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Twiter, MSN Messenger, Yahoo, Skype y otros que determine la Fundación, que tengan como objetivo fines diferentes a las actividades propias de la Fundación.
   c. Uso de marcas, sellos y logos en información escrita o electrónica sin previa autorización.
   d. El intercambio no autorizado de la información institucional con terceros o sus colaboradores.
   e. La descarga, uso, intercambio y/o instalación de aplicaciones que atenten contra la propiedad intelectual, contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica. Así también la descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Jefe respectivo y la Gerencia de Tecnología e Innovación, o a quienes ellos deleguen de forma explícita para esta función.

b) La Fundación realizará inspecciones y monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los colaboradores, así como las actividades realizadas durante la navegación.

c) Cada usuario es garante y responsable de dar uso adecuado a este recurso y en ningún caso deberá ser usado para otro propósito que no sea las obligaciones adquiridas con la Institución, estipuladas en su contrato laboral.

d) Los colaboradores, miembros y terceros, al igual que los empleados o subcontratistas de éstos, no pueden asumir a nombre de FUSALMO, posiciones personales en encuestas de opinión, foros u otros medios similares.

e) Los colaboradores no miembros del Comité de Seguridad envíen o divulguen información a clientes o terceros.

f) Cualquier uso no considerado en las restricciones anteriores, es permitido siempre que se ejecute de manera ética, razonable, responsable, no abusiva y sin afectar la protección de la información de la Fundación, siendo aprobado por el Comité de Seguridad.

15.4 Correo Electrónico

Los colaboradores, miembros y terceros autorizados, a quienes la Fundación les asigne una cuenta de correo electrónico institucional, deberán quedar sujetos a los siguientes lineamientos:
a) La cuenta de correo electrónico debe ser usada para ejecutar, operar y desempeñar las funciones asignadas dentro de FUSALMO, así mismo podrá ser utilizada para uso personal, siempre que se realice en forma ética, razonable, responsable, en concordancia con las buenas prácticas de seguridad de la información relacionadas a la actividad laboral.

b) Los mensajes y la información contenida en los buzones de correo son propiedad de FUSALMO y cada usuario, responsable de su buzón, debe mantener sólo los mensajes relacionados con el desarrollo de sus funciones.

c) La capacidad de los buzones de correo y el tamaño de envío y recepción de mensajes es determinado por la Gerencia de Tecnología e Innovación de acuerdo con las necesidades de cada usuario y previa autorización del Jefe de la dependencia correspondiente.

e) Entre las prohibiciones están enviar cadenas de correo, mensajes con contenido político, racista, sexista, pornográfico, publicitario no institucional o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes que puedan afectar los sistemas internos o de terceros o que vayan en contra de las leyes, la moral y mensajes que inciten a realizar prácticas

ilícitas o promuevan actividades ilegales. No está permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y la Gerencia de Tecnología e Innovación si así se requiere.

f) El envío de información institucional debe ser realizado exclusivamente desde la cuenta de correo autorizada y proporcionada por FUSALMO. De igual modo, las cuentas de correo para uso general no se deben emplear para uso personal.

g) El envío de mensajes publicitarios institucionales deberá ser aprobado por el "Responsable de Comunicaciones" y autorizado por la Dirección Ejecutiva. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico institucional a nombre del remitente y/o servicio habilitado para este fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

h) Toda información institucional, generada con los diferentes programas de software, que requiera ser enviada o compartida fuera de la Fundación y que por sus características de confidencialidad e integridad deba ser protegida, deberá estar en formatos no editable, utilizando las características de seguridad que brindan las herramientas proporcionadas por la Gerencia de Tecnología e Innovación. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer cambios a la información.

i) Todos los mensajes enviados deben respetar el formato estándar e imagen institucional definido por FUSALMO y deben conservar en todos los casos el mensaje legal institucional de confidencialidad.

15.5 Recursos Tecnológicos

FUSALMO reglamenta el adecuado uso de los recursos tecnológicos asignados bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware es exclusiva responsabilidad de la Gerencia de Tecnología e Innovación, siendo los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la Fundación a través de esta gerencia.

b) Los usuarios no están autorizados para realizar cambios relacionados con la configuración del equipo informático que les ha sido asignado, entre ellos:

conexiones de red, usuario del equipo, papel tapiz y protector de pantalla institucional, entre otros. Estos cambios podrán realizarse únicamente por la Gerencia de Tecnología e Innovación.

c) La Gerencia de Tecnología e Innovación debe definir y actualizar la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en los equipos informáticos de los usuarios. De igual modo, realizar el control y verificación de cumplimiento de licenciamiento del respectivo software y aplicaciones.

d) Únicamente los colaboradores, miembros y terceros autorizados por la Gerencia de Tecnología e Innovación, previa solicitud por parte de quien lo requiera, pueden conectarse a la red inalámbrica de la Institución.

e) La sincronización de dispositivos móviles entre los que se pueda realizar intercambios de información con cualquier recurso de la Fundación, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la Gerencia de Tecnología e Innovación y podrá llevarse a cabo sólo en dispositivos provistos por la fundación para este fin. Entre los dispositivos: PDA´s, smartphones, celulares u otros dispositivos electrónicos.

15.6 Clasificación de la Información
[ISO/IEC 27001:2005 A.7.2]

La Institución ha establecido niveles para la clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, u otro medio; con el fin de resguardar la información que pueda ser sujeto de divulgación no autorizada o manipulada erróneamente por parte de sus colaboradores, miembros y terceros.
Por tanto, toda información de la Fundación debe ser identificada, clasificada y documentada de acuerdo con los criterios de clasificación establecidos por el Comité de Seguridad de la Información.

Los niveles de clasificación de la información son:
a) Pública: Colaboradores, miembros, terceros y público en general el acceso a la información.
b) Confidencial: Información para uso interno de la institución y se determinará quién podrá tener acceso a ella.
c) Restringida: Información con acceso único y exclusivo para colaborador y miembros que indispensablemente necesiten la información para el desarrollo de sus actividades y toma de decisiones.

El nivel de clasificación de cada activo de información estará determinado por los propietarios de tales activos tomando en cuenta los criterios de clasificación.

16. SEGURIDAD EN EL RECURSO HUMANO
Ref.: ISO/IEC 27001:2005 A.8

16.1 Responsabilidades del personal
[ISO/IEC 27001:2005 A.8.1.1]

Todos los colaboradores, miembros y terceros que tienen la posibilidad de acceder a la información institucional y a la infraestructura para su procesamiento, son responsables de conocer y cumplir con las políticas y procedimientos establecidos en el Sistema de Gestión de Seguridad de la Información de la Fundación. De igual forma, son responsables de reportar el incumplimiento de las políticas y procedimientos establecidos.
Todos los colaboradores, miembros y terceros deben ser cuidadosos para no divulgar información confidencial en lugares públicos, conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la institución.

16.2 Selección de Personal
[ISO/IEC 27001:2005 A.8.1.2]

Todo proceso laboral realizado por la Institución será regido por las leyes de la Republica de El Salvador, Ley de Equiparación de Oportunidades y lo dispuesto en el Código de Trabajo vigente.
Todo colaborador contratado es seleccionado adecuadamente, se asegura la definición clara de las responsabilidades de éstos y los mecanismos para manejar el incumplimiento de estos requisitos; sin importar el método de contratación, todo colaborador y miembro recibe y acepta las políticas de seguridad de la fundación.
La Institución verificará la información brindada durante el proceso de contratación de los colaboradores; de igual forma, de acuerdo a lo dispuesto en el proceso de selección y contratación de personal y se realiza investigación de antecedentes a todos los candidatos a puestos en la fundación.
La inducción, información de actividades laborales, horarios etc, deberán ser comunicadas al nuevo trabajador a través del Reglamento Interno de Trabajo (autorizado por la Dirección Nacional de Trabajo).

16.3 Términos y Condiciones de Empleo
[ISO/IEC 27001:2005 A.8.1.3]

Todos los colaboradores, miembros y terceros deben aceptar y adoptar las políticas de Seguridad de la Información, así como los términos de uso adecuado

de los recursos de información que le son entregados, previo a la entrega de éstos y teniendo en cuenta que las responsabilidades se extienden fuera de la Institución.

16.4 Capacitación y Entrenamiento en Seguridad de la Información.
[ISO/IEC 27001:2005 A.8.2.2]

La Institución debe garantizar que todos los colaboradores, miembros o terceros que tengan definidas responsabilidades en el Sistema de Gestión de Seguridad de la Información, sean competentes para desempeñar sus funciones y que cuenten con los programas de capacitación y entrenamiento requeridos.
Así también los colaboradores, miembros y terceros, tendrán un proceso de capacitación, dándole a conocer las políticas y compromisos del personal en la seguridad de la fundación y los riesgos conocidos a los que se puede ver expuesta, en caso de incumplimiento.
Los programas de capacitación y educación se encuentran diseñados de manera apropiada y relevante para los roles, responsabilidades y habilidades de las personas que deben asistir a ellos de acuerdo al nivel de información al que tengan acceso y basado en los riesgos a los que estén expuestos.
Todos los procesos de contratación, inducción, capacitación, educación deberán ser registrados y anexarlos a los expedientes de los colaboradores.

6.6.16.5 Procesos Disciplinarios
[ISO/IEC 27001:2005 A.8.2.3]

En el caso de identificarse un incidente de seguridad, éste será registrado e investigado con el fin de determinar las causas y responsables; posteriormente, FUSALMO tomará las acciones disciplinarias para el colaborador, miembro y/o tercero vinculados con el incidente, mediante un proceso disciplinario formal de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la fundación dicho incidente.
Se utilizara la clasificación, tipificación y sanciones clasificadas en el Reglamento Interno de Trabajo (autorizado por la Dirección Nacional de Trabajo)

6.6.16.6 Finalización de Vinculación Laboral o Cambio de Rol
[ISO/IEC 27001:2005 A.8.3]

El responsable de la Unidad de Recursos Humanos, en conjunto con el jefe inmediato del colaborador, miembro y/o responsable del tercero, son los encargados del proceso de finalización de contrato de labores y aseguran que todos los activos propios de la fundación sean devueltos, los accesos físicos y lógicos sean eliminados, y la información pertinente sea respaldada por medio de

un back up, el cual deberá realizarse por un miembro asignado por la Gerencia de Tecnología e Innovación.
En caso de que un colaborador, miembro y/o tercero tenga un cambio de funciones, se debe seguir los mismos procedimientos, en los cuales se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de los mismos de acuerdo a su nueva función.

17. SEGURIDAD FÍSICA Y AMBIENTAL
REF.: ISO/IEC 27001:2005 A.9

17.1 Control de Acceso Físico
[ISO/IEC 27001:2005 A.9.1]

Son áreas de acceso restringido todas aquellas destinadas al procesamiento o almacenamiento de información sensible, en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, por lo que deben contar con medidas de control de acceso físico mediante perímetro de seguridad, tales que puedan ser auditadas; así también contar con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.
Los centros de cómputo, cableado y áreas técnicas de las oficinas, deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales, especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones; es así como se velara por el cumplimiento de la normativa OHSAS 18000 de Seguridad y Salud Ocupacional en las Empresas, en aspectos como prevención de riesgos laborales y seguridad en estructuras organizativas e instalaciones.
Deben controlarse las áreas de carga, descarga, entrega de mercancías y demás puntos de acceso a las instalaciones y en lo posible separarlas de las áreas seguras para evitar el acceso no autorizado.
Los colaboradores, así como los visitantes, deben portar identificación visible mientras permanezcan dentro de las instalaciones de la Fundación; así mismo, deben revisarse, actualizarse y monitorearse periódicamente los privilegios de acceso a las áreas seguras y restringidas de la Institución.

17.2 Protección y Ubicación de los Equipos
[ISO/IEC 27001:2005 A.9.2]

La infraestructura tecnológica, que incluye servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas y eléctricas, así como estaciones de trabajo y

dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden soporte y aseguren que la información crítica de las dependencias puedan ser ubicados y protegidos a fin de prevenir la pérdida, daño, robo o acceso no autorizado a los mismos. Además, deben alejarse de sitios que puedan tener riesgo de amenazas incendio, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros. Los colaboradores y subcontratistas, no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos a que tengan acceso como parte de la infraestructura tecnológica.
La Institución por medio de mecanismos adecuados monitoreará las condiciones ambientales y temperatura de las zonas donde se encuentren los equipos (Centros de Cómputo), así como sistemas de protección y equipos contra incendios según cada riesgo por área acorde a lo definido en la Asociación Nacional de Protección contra el fuego (ingles: National Fire Protection Association NFPA)
Además, proveerá suministros y equipamiento de soporte que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información, ante una falla en el suministro, con el fin de evitar la pérdida o corrupción de información. Estos suministros serán monitoreados, revisados y medidos permanentemente para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños; por otra parte, debe establecer un programa de planeación y ejecución de mantenimientos preventivos a la infraestructura tecnológica.

17.3 Retiro y seguridad de equipos y medios de información fuera de las instalaciones.
[ISO/IEC 27001:2005 A.9.2.5; A.9.2.7]

Todos los colaboradores son responsables de velar por la seguridad de los equipos que se encuentren fuera de sus instalaciones:

a) En ningún caso los equipos informáticos, que estén siendo transportados en un vehículo, pueden ser dejados en lugares públicos; excepto que haya un responsable directo.
b) Los equipos de infraestructura deben transportarse bajo medidas de seguridad apropiadas que garanticen la integridad física de los dispositivos.
c) Los equipos portátiles siempre deben transportarse como equipaje de mano y tener especial cuidado de no exponerlos a campos electromagnéticos.
d) Los equipos deberán contar con un seguro que los proteja de robo.
e) En caso de robo o pérdida deberá informarse inmediatamente a la Gerencia de Tecnología e Innovación para que se inicie el trámite interno y deberá poner la denuncia ante la autoridad competente.

f) La salida de los equipos debe ser autorizada y registrada, de tal manera que se detallen los datos técnicos y otros datos importantes para identificación de equipo entregado, de igual forma se utilizara esta información en el momento de retorno del mismo.

El retiro de equipo informático o sus periféricos, dispositivos de almacenamiento, software e información crítica fuera de las instalaciones de la Fundación debe realizarse en base a los procedimientos establecidos por la Dirección Ejecutiva y la Gerencia de Tecnología e Innovación.

17.4 Eliminación o Reutilización Segura de Equipos y Medios [ISO/IEC 27001:2005 A.9.2.6]

La Institución debe identificar los riesgos relacionados con la destrucción, reparación o eliminación de equipos y medios de almacenamiento; para ello debe definir e implementar mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura.
Para el equipo que sea reasignado o dado de baja, se realizará una copia de respaldo de la información, luego el equipo será sometido a un proceso de eliminación segura de la información sensible almacenada y del software instalado, con el propósito de evitar la fuga de información y/o recuperación no autorizada de la misma.
Los equipos dados de baja en buen estado pueden ser donados a otras instituciones, asegurando que no lleve información o programas con licencia que pertenecen a la fundación. En el caso sean para destrucción o reciclaje de partes se deben buscar empresas o mecanismos que minimicen la contaminación al medio ambiente.

18. GESTIÓN DE COMUNICACIONES Y OPERACIONES
Ref.: ISO/IEC 27001:2005 A.10

18.1 Documentación de Procedimientos Operativos [ISO/IEC 27001:2005 A.10.1.1]

Con el propósito de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica, se dispondrá de procedimientos, registros e instructivos de trabajo debidamente documentados y actualizados. Cada procedimiento tendrá un responsable para su definición y mantenimiento y debe garantizar la disponibilidad del mismo.

18.2 Control de Cambios
[ISO/IEC 27001:2005 A.10.1.2]

Los cambios realizados sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica deben ser controlados, gestionados, autorizados adecuadamente y sometidos a una evaluación que permita identificar riesgos asociados que pueden afectar la operación del negocio, de acuerdo con los lineamientos de gestión de cambios.
El Comité de Seguridad deberá revisar todo cambio estructural que se proyecte realizar sobre las plataformas críticas, estableciendo además los requerimientos de seguridad necesarios, conforme a las políticas establecidas y con el fin de evitar un impacto adverso en las operaciones del negocio.

18.3 Segregación de Funciones
[ISO/IEC 27001:2005 A.10.1.3]

Toda tarea en la que los colaboradores requieran acceso a la infraestructura tecnológica y a los sistemas de información, debe estar claramente definida en cuanto a roles y responsabilidades, así como el nivel de acceso y los privilegios correspondientes; esto con el propósito de reducir y evitar el uso no autorizado o modificación sobre los activos de información.

Por tanto:

a) Deberán implementarse las reglas de acceso a todos los sistemas de disponibilidad crítica, de modo que haya segregación de funciones entre quien administre, opere, mantenga, audite y tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

b) Los módulos ejecutables no deberán trasladarse directamente de las librerías de prueba a las librerías de producción sin que previamente éstos hayan sido compilados por el área asignada para tal efecto; además, esta área asignada en ningún momento deberá ser la misma que se utiliza para el desarrollo y producción.

c) El nivel de administrador en los sistemas y equipo debe tener un control, de modo que exista una supervisión a las actividades realizadas en éstos por parte del administrador del sistema.

d) Deben segregarse las funciones de soporte técnico, planificadores y operadores.

18.4 Separación de los Ambientes de Desarrollo, Prueba y Producción [ISO/IEC 27001:2005 A.10.1.4]

En la Institución se definen diferentes ambientes para la ejecución de actividades de desarrollo, pruebas y puesta en producción de sus aplicaciones, esto con el fin de garantizar la integridad de la información procesada y evitar interferencias en el desempeño y seguridad de cada uno de los ambientes.

De modo que se definen los siguientes ambientes:

a) Ambiente de Desarrollo: hardware y software donde se ubican los recursos informáticos necesarios para efectuar tareas relacionadas con la generación o modificación de aplicaciones, entre otros.

b) Ambiente de Prueba: hardware y software que soportan los sistemas de información, los cuales son utilizados para verificar la funcionalidad del desarrollo de éstos y sus aplicativos, para realizar los ajustes necesarios antes de ser puestos en funcionamiento en el ambiente de producción.

c) Ambiente de Producción: hardware y software que soportan los sistemas de información utilizados por los colaboradores para la ejecución de las operaciones.

A través de las políticas de control de acceso físico y lógico definidas, se controla cada uno de los ambientes; mientras que los ambientes de desarrollo, pruebas y producción deben estar separados, tener su propia plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, para evitar que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.
La Gerencia de Tecnología e Innovación debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para evitar el acceso y cambios no autorizados; además, debe asegurar que los usuarios dispongan de diferentes perfiles para el ambiente de desarrollo, pruebas y de producción, así como también que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

6.6.18.5 Gestión de la Capacidad [ISO/IEC 27001:2005 A.10.3.1]

La Institución, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada, realizará un proceso continuo de

monitoreo, análisis y evaluación del rendimiento y capacidad de la infraestructura tecnológica de procesamiento de información.
Se realizarán mediciones de la infraestructura tecnológica, en relación a las variables críticas de operación, con el objetivo de verificar el estado y uso de los recursos de tal modo de definir proyecciones de crecimiento que aseguren la integridad de procesamiento y disponibilidad de la infraestructura. Los resultados de estas mediciones serán analizados y presentados al Comité de Seguridad y, en caso de ser necesario, se planificará la adquisición de nuevos recursos o elementos para soportar la demanda.

18.6 Aceptación de Sistemas
[ISO/IEC 27001:2005 A.10.3.2]

La Gerencia de Tecnología e Innovación asegurará que los requerimientos, criterios funcionales y técnicos para la aceptación de nuevos sistemas, actualizaciones o nuevas versiones de software, sean claros y definidos, así como documentados y aprobados acorde a las necesidades de la Institución. Éstos deberán migrarse al ambiente de producción, sólo después de haber sido formalmente probados.

18.7 Protección Contra Software Malicioso
[ISO/IEC 27001:2005 A.10.4]

Los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, anti spam, anti spyware y otras aplicaciones que brindan protección contra código malicioso, contando con los controles adecuados para detectar, prevenir y recuperar posibles daños causados por código móvil y malicioso. La Gerencia de Tecnología e Innovación autorizará el uso de las herramientas y asegurará que éstas y el software de seguridad, no sean deshabilitados bajo ninguna circunstancia, así como su actualización permanente.

Así mismo, no está permitido:

a) La desinstalación y/o desactivación de software y herramientas de seguridad aprobadas previamente.

b) Escribir, generar, compilar, copiar, propagar, ejecutar o introducir cualquier código de programación diseñado para dañar o afectar el desempeño de cualquier infraestructura tecnológica.

c) El uso de código móvil, siempre que no sea utilizado en base a las políticas y normas de seguridad definidas o debidamente autorizado por la Gerencia de Tecnología e Innovación.

18.8 Copias de Respaldo
[ISO/IEC 27001:2005 A.10.5]

La Institución debe asegurar que la información con cierto nivel de clasificación contenida en su plataforma tecnológica, sea periódicamente resguardada mediante mecanismos y controles que garanticen su identificación, protección, integridad y disponibilidad; adicionalmente, se debe establecer un plan de restauración de copias de seguridad que sean probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia.
La Gerencia de Tecnología e Innovación establecerá procedimientos para el resguardo y recuperación de la información, deberá incluir especificaciones acerca del traslado, frecuencia e identificación de la misma, así como los períodos de retención; además, deberá disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
El sitio donde se resguardan las copias de seguridad, debe tener los controles de seguridad adecuados y cumplir con máximas medidas de protección y seguridad física. Lo anterior se debe realizar de acuerdo con lo establecido en el procedimiento Copia de Respaldo (Back up).

18.9 Gestión de Medios Removibles
[ISO/IEC 27001:2005 A.10.7]

La Gerencia de Tecnología e Innovación implementará los controles necesarios para asegurar que en los sistemas de información sólo los colaboradores autorizados pueden hacer uso de los medios de almacenamiento removibles. Así mismo, el colaborador se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información que esté contenida en ellos.

18.10 Intercambio de Información
[ISO/IEC 27001:2005 A.10.8]

La Información firmará acuerdos de confidencialidad con los colaboradores, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial; estos acuerdos especifican las responsabilidades para el intercambio de información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de la información.

Todo colaborador de la Institución es responsable de proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de medios para el intercambio de información que pueda generar una divulgación o modificación no autorizada de la misma, cuyo uso aceptable se especifica en la política sobre el uso adecuado de los activos (15.2).
Son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la información, los propietarios de la información que se quiere intercambiar, y son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad requeridos; así como ser los custodios de esta información.

18.11 Comercio y Transacciones Electrónicas
[ISO/IEC 27001:2005 A.10.9]

Para el desarrollo de actividades de comercio y transacciones electrónicas, se deben definir y establecer mecanismos para generar conexiones y transferencias de información seguras, de acuerdo con las regulaciones aplicables.
Se deben establecer los requerimientos necesarios para proporcionar a los usuarios la información pertinente sobre las transacciones en línea, tal como las condiciones y costos de la transacción, así como las medidas de seguridad pertinentes; para ello se debe extender un reporte, en papel o por medios electrónicos, al momento de la realización de cada transacción.

18.12 Monitoreo del Uso de los Sistemas
[ISO/IEC 27001:2005 A.10.10]

Para garantizar la seguridad de la información, debe brindar los mecanismos y controles para detectar las actividades de procesamiento de información no autorizadas.
Se deben generar archivos de registro de eventos definidos por los responsables de la administración de las aplicaciones que hacen parte de la infraestructura en el procesamiento de la información, comunicaciones y seguridad.
A partir de la metodología de análisis de riesgos de seguridad de la información, debe identificar el nivel de monitoreo requerido para las aplicaciones y dispositivos tecnológicos y establecer los controles necesarios para la mitigación de tales riesgos. Si en el proceso de la revisión de los archivos de registro de eventos se evidencia la ocurrencia de un incidente de seguridad, se determinará el nivel de criticidad del mismo y se seguirán las disposiciones definidas en el procedimiento de reporte y seguimiento de incidentes de seguridad.
Todos los registros de auditoría de los sistemas de información sólo mantendrán privilegios de lectura y, a través de la definición de perfiles de usuario, serán protegidos de accesos y modificaciones no autorizadas.

Todos los relojes de los sistemas informáticos deben estar sincronizados, con el fin de lograr un control apropiado de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes.

19. CONTROL DE ACCESO
Ref.: ISO/IEC 27001:2005 A.11

19.1 Control de Acceso Lógico
[ISO/IEC 27001:2005 A.11.1]

El acceso a plataformas, aplicaciones, servicios y a cualquier recurso de información será asignado de acuerdo a la identificación de requerimientos de seguridad y del negocio que definan las diferentes dependencias, así como normas legales o leyes aplicables a la protección de acceso a la información en los sistemas.
Los accesos a plataformas, usuarios y segmentos de red son asignados por los responsables de la administración de la infraestructura tecnológica en base a procesos formales de autorización, los cuales deben ser revisados de manera periódica por la Gerencia de Tecnología e Innovación.
Además, la dependencia propietaria de la información, o quien ésta defina, debe autorizar el acceso a los sistemas de acuerdo con el nivel de clasificación de la misma, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los colaboradores y terceros. Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos, independientemente si el acceso es por Internet, acceso telefónico o por otro medio.

19.2 Gestión de Contraseñas de Usuario
[ISO/IEC 27001:2005 A.11.2.3]

Los recursos de información críticos tienen privilegios de acceso de usuarios en base a los roles y perfiles que cada colaborador requiera para el desarrollo de sus funciones; éstos son definidos y aprobados por las áreas de negocio y administrados por la Gerencia de Tecnología e Innovación. Es responsabilidad de ésta última la creación, modificación y eliminación de usuarios y contraseñas en la infraestructura de procesamiento de Información.
Todo colaborador o tercero que requiera tener acceso a los sistemas debe estar debidamente autorizado y acceder a dichos sistemas haciendo uso como mínimo de un usuario y contraseña asignado. El colaborador debe ser responsable y garantizar el buen uso de las credenciales de acceso asignadas.

19.3 Escritorios y Pantallas Limpias

Todos los colaboradores deben proteger la información de carácter restringida o confidencial cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales, esto con el fin de evitar pérdidas, daños o accesos no autorizados a la información. La medida incluye documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles. Así también la información que se envía a las impresoras centralizadas, deberá recuperarse de manera inmediata.
Los colaboradores son responsables de bloquear la sesión de trabajo en el momento en que se retiren, ésta podrá desbloquearse sólo con la contraseña del usuario y cuando finalicen las actividades; se deben cerrar todas las aplicaciones y dejar los equipos apagados.
Únicamente está autorizado el uso de papel tapiz y el protector de pantalla institucional en los equipos informáticos; este se activará automáticamente después de cinco minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

19.4 Segregación de Redes [ISO/IEC 27001:2005 A.11.4.5]

Se debe separar en segmento de red físico y lógico e independiente de los segmentos de red de usuarios, conexiones de redes con terceros y del servicio de acceso a Internet, la plataforma tecnológica que soporta los sistemas de información. La división de estos segmentos debe realizarse por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere.
La Gerencia de Tecnología e Innovación es la responsable de establecer el perímetro de seguridad necesario para proteger los segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
Como medio de autenticación de conexiones, se debe establecer mecanismos de identificación automática de equipos en la red, lo cual deberá realizarse desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información.
Los administradores de recursos tecnológicos son responsables de garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soportan los sistemas de información, estén siempre restringidos y monitoreados para así prevenir accesos no autorizados.

19.5 Computación Móvil
[ISO/IEC 27001:2005 A.11.7.1]

Los equipos portátiles podrán ser utilizados fuera de las instalaciones de la institución sólo en los casos que los usuarios hayan sido autorizados por la Gerencia de Tecnología e Innovación, previa solicitud de la dependencia respectiva y éstos deberán protegerse mediante el uso de controles tecnológicos, tales como:

a) Antivirus.
b) Cifrado de datos.
c) Restricción en la ejecución de aplicaciones.
d) Entre otros.

La sincronización de dispositivos móviles con cualquier sistema de información de FUSALMO, será autorizado por la Gerencia de Tecnología e Innovación y la dependencia respectiva.

19.6 Teletrabajo
[ISO/IEC 27001:2005 A.11.7.2]

El acceso a la información desde redes externas, podrá realizarse remotamente mediante autenticación, uso de conexiones seguras y asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede, con previa autorización de la Gerencia de Tecnología e Innovación.

20. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE INFRAESTRUCTURA TECNOLÓGICA
Ref.: ISO/IEC 27001:2005 A.12

20.1 Identificación de Requerimientos de Seguridad
[ISO/IEC 27001:2005 A.12.1.1]

Toda incorporación de nuevos dispositivos de hardware o software, ya sea de desarrollo interno o externo y cambios y/o actualizaciones a los sistemas; deben contar con la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, bajo la responsabilidad de la Gerencia de Tecnología e Innovación y las dependencias propietarias del sistema.
Los requerimientos de seguridad de la información u otras obligaciones, deben quedar establecidos en los acuerdos contractuales que se realicen entre la Institución y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Por tanto, será responsabilidad de la Gerencia de Tecnología e Innovación, garantizar la definición y cumplimiento

de los requerimientos de seguridad y con la Dirección Ejecutiva deben establecer tales aspectos en las obligaciones contractuales específicas.

20.2 Controles Criptográficos [ISO/IEC 27001:2005 A.12.3.1]

Se establece el uso de protocolos y controles criptográficos para el uso en aplicativos, transferencia de información, enlaces de comunicaciones, protección de medios y acceso remoto; con el fin de proteger la confidencialidad, integridad y disponibilidad de la información. Además, no se permite el uso de herramientas o mecanismos de encriptación de información diferentes a los autorizados.

20.3 Seguridad de los Sistemas [ISO/IEC 27001:2005 A.12.4]

No se permite la instalación de herramientas de desarrollo ni programas fuente en los sistemas de producción, por lo que las nuevas aplicaciones, desarrollos, y/o sistemas operativos o modificaciones a éstos, que dan soporte a los sistemas de información, deberán ser implementados en el ambiente de producción después de un protocolo de pruebas que involucre aspectos funcionales, de seguridad, de compatibilidad con otros sistemas de información y facilidad de uso. Todo ello con el fin de minimizar el riesgo de corrupción de los sistemas de información que se encuentran en producción.

Los administradores de las plataformas de producción son los responsables de coordinar y/o ejecutar las actualizaciones programadas, así como de controlar el acceso y uso de los programas fuente y/o de las aplicaciones que operan en ellas.

Los proveedores de desarrollo de software no deben tener acceso directo a los sistemas de información en el momento de hacer la transición a producción; siendo esta actividad, responsabilidad del administrador de la plataforma que corresponde.

No se permitirá copiar información confidencial desde el ambiente de producción al ambiente de prueba y de ser así, debe garantizarse que los datos reales son mezclados aleatoriamente sin que ello afecte la estructura funcional de la solución.

En los sistemas de producción no se permite el uso de versiones de software no soportados por el fabricante y el uso de versiones de prueba no liberadas al mercado, éstas serán autorizadas por la Gerencia de Tecnología e Innovación, quienes mantendrán actualizado el inventario de software autorizado.

20.4 Gestión de Vulnerabilidades Técnicas [ISO/IEC 27001:2005 A.12.6]

La Gerencia de Tecnología e Innovación es responsable de identificar las vulnerabilidades técnicas de las plataformas tecnológicas, de comunicaciones y seguridad que soporten los sistemas de información críticos. A su vez, el personal que administra esta plataforma tecnológica, es responsable de verificar periódicamente la información publicada por parte de los fabricantes y foros de seguridad en relación a nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información.
Deben realizarse, por lo menos una vez al año, pruebas de vulnerabilidades para las plataformas críticas, las cuales deben ser desarrolladas por un ente independiente al área objeto de pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
Las medidas correctivas que requieran ser aplicadas en las plataformas tecnológicas, como resultado de la identificación de vulnerabilidades técnicas, serán responsabilidad del personal que administre la infraestructura tecnológica, de comunicaciones y seguridad.
La Gerencia de Tecnología e Innovación será responsable del seguimiento y verificación de la identificación de las causas que generaron las vulnerabilidades y las acciones de corrección pertinentes.

21. GESTIÓN DE INCIDENTES DE SEGURIDAD Ref.: ISO/IEC 27001:2005 A.13

21.1 Comunicación de Incidentes y Eventos de Seguridad de la Información [ISO/IEC 27001:2005 A.13.1]

Un evento de seguridad es la ocurrencia de una situación que indica una posible violación a las políticas de seguridad de la información o fallas en los controles, que no genere un impacto en el desarrollo de las operaciones de la entidad y que puede ser controlado rápidamente. Por otro lado, un incidente de seguridad de la información, conlleva a la ocurrencia de un acto intencional o no intencional que tiene una alta probabilidad de afectar el buen funcionamiento de los sistemas de información, o en todo caso, que a causa de este acto se vea afectada la operación y amenaza la seguridad de la información.
Por tanto, los colaboradores y/o terceros deben reportar, realizando lo indicado en el procedimiento de reporte y seguimiento de incidentes de seguridad, cualquier situación que se pueda considerar como un evento de seguridad y que comprometa la preservación de la confidencialidad, disponibilidad y/o integridad de la información; será responsabilidad del Comité de Seguridad de la Información,

determinar si la situación reportada corresponde a un evento o a un incidente de seguridad y en base a ello ejecutar las acciones necesarias según el caso.
La Dirección Ejecutiva o a quien éste delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades, y representan el único canal de comunicación autorizado para hacer pronunciamientos oficiales ante entidades externas. Por tanto, si alguien no autorizado lleva a cabo tareas relacionadas con esta actividad, será interpretado como incumplimiento de las políticas establecidas.

21.2 Manejo de Incidentes de Seguridad [ISO/IEC 27001:2005 A.13.2]

El Comité de Seguridad de la Información o a quien designe, es la única figura autorizada, para evaluar las debilidades o incidentes de seguridad reportados; por tanto, debe asignar un responsable o grupo de personas responsables de realizar la investigación y seguimiento a los eventos de seguridad reportados, el cual recibirá el nombre de Grupo de Atención de Incidentes, quienes deberán informar al Comité de Seguridad tales resultados, pudiendo requerir en el proceso, el apoyo de otras áreas de la institución o de entidades externas.
El Comité de Seguridad de la Información deberá mantener registros de las anomalías o debilidades que le sean reportadas y que amenacen la seguridad de la información; además, deben asegurar el registro de los incidentes tomando en cuenta las causas, impacto, frecuencia y forma de solución, con el propósito de mantener estadísticas anuales de comportamiento de respuesta ante incidentes, generar aprendizajes de lo ocurrido e implementar mejoras en las acciones de control y políticas según se requiera.
Es responsabilidad de todos los involucrados, preservar la confidencialidad de la información relacionada con el manejo, investigación y seguimiento de los incidentes de seguridad de la información.
La Institución establecerá los mecanismos de control para recopilar y preservar la evidencia de acciones que vayan en contra de la información crítica y que deban ser objeto de acciones disciplinarias; por otro lado, las actividades que generen sospecha de mal uso de la información, deberán registrarse como evidencia en la aplicación de sanciones acordes al impacto causado.

22. ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO
Ref.: ISO/IEC 27001:2005 A.14

22.1 Seguridad de la Información en la Continuidad del Negocio [ISO/IEC 27001:2005 A.14.1.1]

Ante la ocurrencia de eventos no previstos o desastres naturales, se debe contar con un plan documentado, aprobado y actualizado, que garantice la continuidad de las operaciones y de los procesos críticos; se debe establecer un plan de recuperación tecnológica que defina las directrices y lineamientos mínimos requeridos para recuperar y restablecer las operaciones de los servicios de tecnología, así como los requerimientos de seguridad, funciones y responsabilidades relacionados con el plan.

22.2 Análisis de Riesgo e Impacto del Negocio [ISO/IEC 27001:2005 A.14.1.2]

La Institución debe realizar un análisis de riesgos y su impacto en el negocio, en base a las buenas prácticas, con el fin de definir un plan de continuidad del negocio y recuperación de desastres; éstas actividades deberán ser ejecutadas al menos una vez al año o ante cambios importantes en la misma.

22.3. Declaración de Desastre y Activación de los Planes de Continuidad del Negocio [ISO/IEC 27001:2005 A.14.1.3]

La declaración de desastre ante los líderes de los equipos de recuperación, implica el inicio de las actividades descritas en el plan de continuidad del negocio para cada uno de éstos.
Por lo que será necesario definir quiénes serán los responsables de declarar un desastre, así como los voceros autorizados para definir el inicio de una contingencia dentro de la Institución y una vez dada esta autorización de inicio, comenzarán a ejecutarse cada una de las actividades definidas en el plan de continuidad del negocio y de recuperación de desastres.

22.4 Entrenamiento y Capacitación [ISO/IEC 27001:2005 A.14.1.4]

Los colaboradores y terceros relacionados con la Institución, deben ser entrenados en sus roles y responsabilidades asignados en el plan de continuidad del negocio.

22.5 Pruebas y Mantenimiento del Plan de Continuidad [ISO/IEC 27001:2005 A.14.1.5]

Deberán realizarse pruebas al plan de continuidad del negocio, por lo que se definirá un área responsable de coordinar periódicamente estas pruebas y mantener el plan actualizado, de acuerdo con las necesidades y requerimientos de la Fundación.

23. CUMPLIMIENTO DE LOS REQUERIMIENTOS
Ref.: ISO/IEC 27001:2005 A.15

23.1 Cumplimiento de Requerimientos
[ISO/IEC 27001:2005 A.15.1.1]

La Institución deberá cumplir con la legislación aplicable de las leyes salvadoreñas, las regulaciones emitidas por organizaciones de control gubernamentales o no gubernamentales que apliquen, además de las obligaciones contractuales con terceros; por ello, debe documentarse estos requerimientos para cada sistema de información.
La Asesoría Jurídica es la responsable de orientar a la Fundación acerca de los requisitos normativos y regulatorios emitidos por organizaciones de control, así como de las obligaciones con terceros y colaboradores, enmarcados en del cumplimiento de la legislación salvadoreña vigente.

23.2 Derechos de Propiedad Intelectual
[ISO/IEC 27001:2005 A.15.1.2]

Se dará cumplimiento a la reglamentación de propiedad intelectual vigente en el país y ejecutará revisiones periódicas para garantizar que se están respetando los derechos de propiedad intelectual, los cuales incluyen licencias de código fuente, documentos que son parte del conocimiento del negocio, propuestas comerciales, patentes, información publicitaria y comercial relacionada con la imagen institucional.
Se define a la Gerencia de Tecnología e Innovación, como responsable de mantener y administrar el inventario y control de las licencias de software, hardware y aplicaciones utilizadas en la Institución, además de los medios y contratos que se relacionan con la actividad comercial de compra de software y hardware; además, está prohibido el uso de software ilegal o no licenciado, por lo que los colaboradores serán sancionados por la instalación y utilización de software no autorizado en sus estaciones de trabajo y en las plataformas tecnológicas que soportan los sistemas de información.

Los acuerdos contractuales entre la Institución y cualquier proveedor de desarrollo de software, deben especificar claramente los compromisos de preservación de los derechos de propiedad intelectual y todos los programas de software utilizados en el desarrollo de las operaciones del negocio, deben incluir los avisos de información de derechos de autor correspondientes y mostrarse cuando el usuario inicia la aplicación.

23.3 Protección de Registros [ISO/IEC 27001:2005 A.15.1.3]

Dado que la Institución se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requerimientos normativos, legales o regulatorios de pérdida, destrucción o falsificación; éstos estarán identificados en un listado maestro de registros y serán protegidos en base al nivel de clasificación, cumpliendo con la legislación salvadoreña vigente, se determina que la información personal de los colaboradores y/o contratistas es de carácter confidencial, por lo que también se implementarán los controles para su protección y no divulgación a terceras partes, caso contrario si se cuenta con la autorización formal del colaborador y/o contratista o en los casos en que las regulaciones lo permitan.

PROCEDIMIENTO DE RESPALDO DE LA INFORMACIÓN (Back Up)

Preparado por	
Nombre	Firma
Puesto	Fecha

Revisado por			
Propietario		Director (si aplica)	
Nombre	Firma	Nombre	Firma
Puesto	Fecha	Puesto	Fecha

Aprobado por	
Nombre	Firma
Puesto	Fecha

Copia controlada	
Titular	Copia número
El propietario del procedimiento es el responsable de la revisión anual, actualizaciones, monitoreo, control y la aprobación de este procedimiento.	

PROCEDIMIENTO DE RESPALDO DE LA INFORMACIÓN (Back Up)

1. OBJETIVO

Establecer los lineamientos y procedimientos para realizar el respaldo de información de los servidores.

2. ALCANCE

2.1 Inclusiones

Este documento describe los procedimientos de respaldo y recuperación para los sistemas, incluyendo aplicaciones, bases de datos, sistemas operativos, archivos de usuarios en los servidores y configuración de dispositivos de FUSALMO, los cuales son administrados por la Coordinación de Servicios Tecnológicos de la Gerencia de Tecnología e Innovación.

2.2 Exclusiones

No se incluye todos aquellos procesos de respaldo y recuperación llevados a cabo por terceros.

No se incluyen los procesos de respaldo y recuperación de las computadoras personales de los usuarios finales de la Fundación.

3. DEFINICIONES

3.1 Respaldo (Backup)

Acción de realizar una copia de datos de un servidor a un medio de almacenamiento (Disco óptico) como prevención en caso de pérdida total o daño parcial de la fuente original de estos datos.

3.2 Recuperación

Consiste en la acción de recuperar los datos que han sido previamente copiados a un medio de almacenamiento.

4. RESPONSABILIDAD

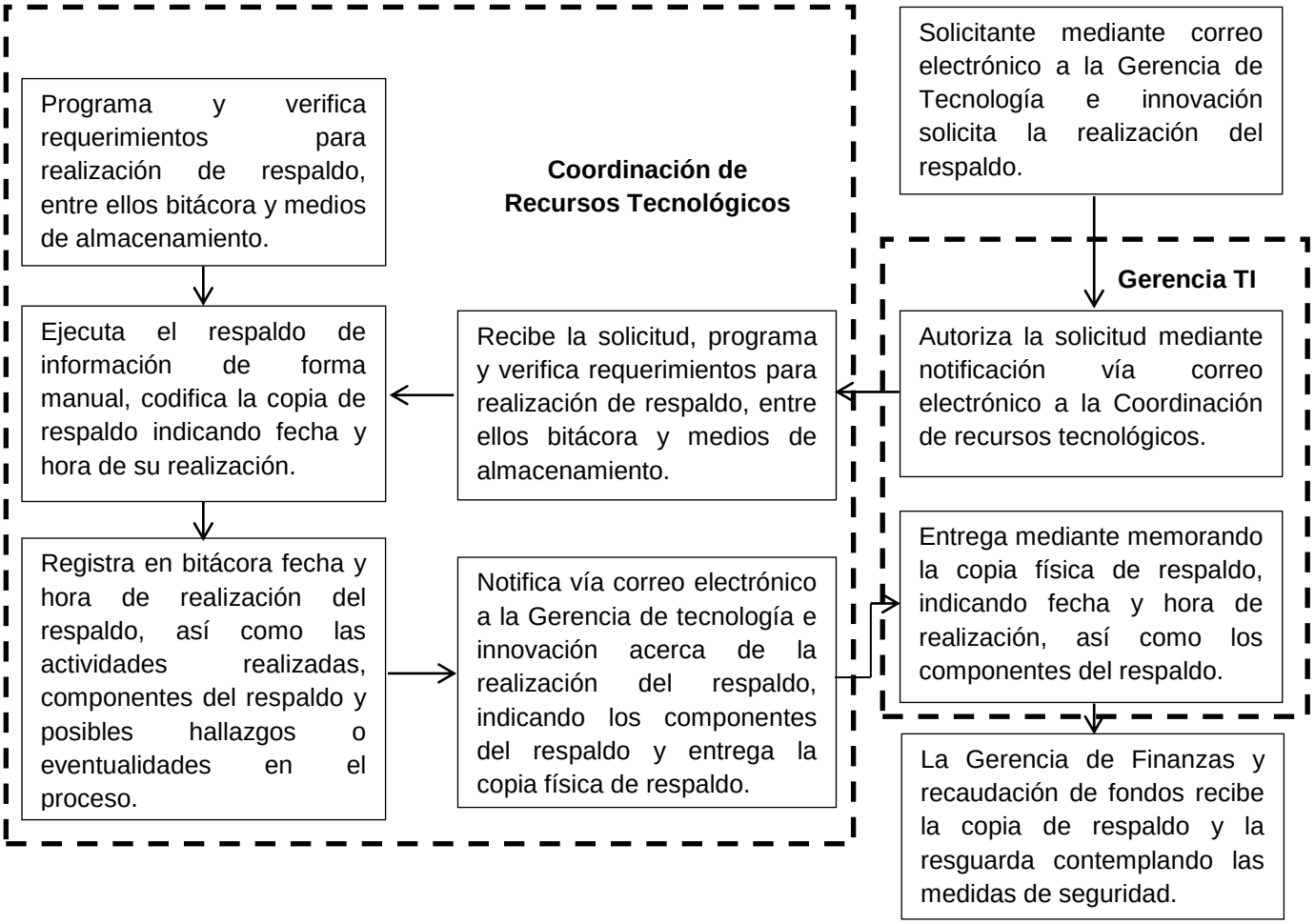
Es responsabilidad del Coordinador de Recursos Tecnológicos, establecer los mecanismos necesarios y ejecutarlos, para la realización de los respaldos en los medios establecidos.

5. DESCRIPCIÓN DEL PROCEDIMIENTO DE RESPALDO

No.	Responsable	Actividad
1	Coordinación de Recursos Tecnológicos	El respaldo de información clasificada se realiza semanalmente en forma programada cada viernes. El Coordinador de recursos tecnológicos programa y verifica requerimientos para realización de respaldo, entre ellos bitácora y medios de almacenamiento. Continuar con el paso 5. Si el respaldo es solicitado por una de las partes interesadas, continuar con el paso 2.
2	Solicitante	El respaldo de información se realiza en base a solicitud o de forma programada. Este puede ser solicitado por las partes interesadas: Gerencia de finanzas y recaudación de fondos, Gerencia de tecnología e innovación, Dirección Ejecutiva. El interesado mediante correo electrónico a la Gerencia de Tecnología e innovación solicita la realización del respaldo.
3	Gerencia de Tecnología e Innovación	Autoriza la solicitud mediante notificación vía correo electrónico a la Coordinación de recursos tecnológicos.

No.	Responsable	Actividad
4	Coordinación de Recursos Tecnológicos	Recibe la solicitud, programa y verifica requerimientos para realización de respaldo, entre ellos bitácora y medios de almacenamiento.
5	Coordinación de Recursos Tecnológicos	Ejecuta el respaldo de información de forma manual, almacenando las carpetas de información correspondientes en el medio de almacenamiento. Codifica la copia de respaldo indicando fecha y hora de su realización.
6	Coordinación de Recursos Tecnológicos	Registra en bitácora fecha y hora de realización del respaldo, así como las actividades realizadas, componentes del respaldo y posibles hallazgos o eventualidades en el proceso.
7	Coordinación de Recursos Tecnológicos	Notifica vía correo electrónico a la Gerencia de tecnología e innovación acerca de la realización del respaldo, indicando los componentes del respaldo y entrega la copia física de respaldo.
8	Gerencia de Tecnología e Innovación	Entrega mediante memorando a la Gerencia de Finanzas y recaudación de fondos, la copia física de respaldo, indicando fecha y hora de realización, así como los componentes del respaldo.
9	Gerencia de Finanzas y Recaudación de Fondos	Recibe la copia de respalda y la resguarda contemplando las medidas de seguridad correspondientes.

6. DIAGRAMA DEL PROCEDIMIENTO DE RESPALDO



PROCEDIMIENTO DE REPORTE Y SEGUIMIENTO DE INCIDENTES DE SEGURIDAD.

Preparado por	
Nombre	Firma
Puesto	Fecha

Revisado por			
Propietario		Director (si aplica)	
Nombre	Firma	Nombre	Firma
Puesto	Fecha	Puesto	Fecha

Aprobado por	
Nombre	Firma
Puesto	Fecha

Copia controlada	
Titular	Copia número
El propietario del procedimiento es el responsable de la revisión anual, actualizaciones, monitoreo, control y la aprobación de este procedimiento.	

PROCEDIMIENTO DE REPORTE Y SEGUIMIENTO DE INCIDENTES DE SEGURIDAD.

1. OBJETIVO

Definir las acciones por medio de las cuales los problemas e incidentes, relacionados con tecnología de información, son reportados, registrados, investigados, diagnosticados, valorados y resueltos. El procedimiento asegura que los problemas son asignados a un responsable, se les da seguimiento y son monitoreados durante todo su ciclo de vida.

2. ALCANCE

2.1 Inclusiones

Este procedimiento aplica a todos los problemas e incidentes en las aplicaciones, bases de datos, sistemas operativos, centros de datos y componentes de red en la infraestructura de FUSALMO, dichos incidentes o problemas son reportados a LA Gerencia de Tecnología e Innovación y debidamente registrados para su seguimiento.

2.2. Exclusiones

No se han identificado exclusiones para este procedimiento.

3. DEFINICIONES

3.1 Software

Aplicaciones, programas o sistemas computacionales.

3.2. Hardware

Componentes físicos de tecnología, en este caso tecnología de la información.

4. RESPONSABILIDAD

Es responsabilidad del Coordinador de Recursos Tecnológicos, establecer los mecanismos necesarios y ejecutarlos, para dar soporte a las aplicaciones o servicios de TI y de resolver los problemas o incidentes que le hayan sido asignados.

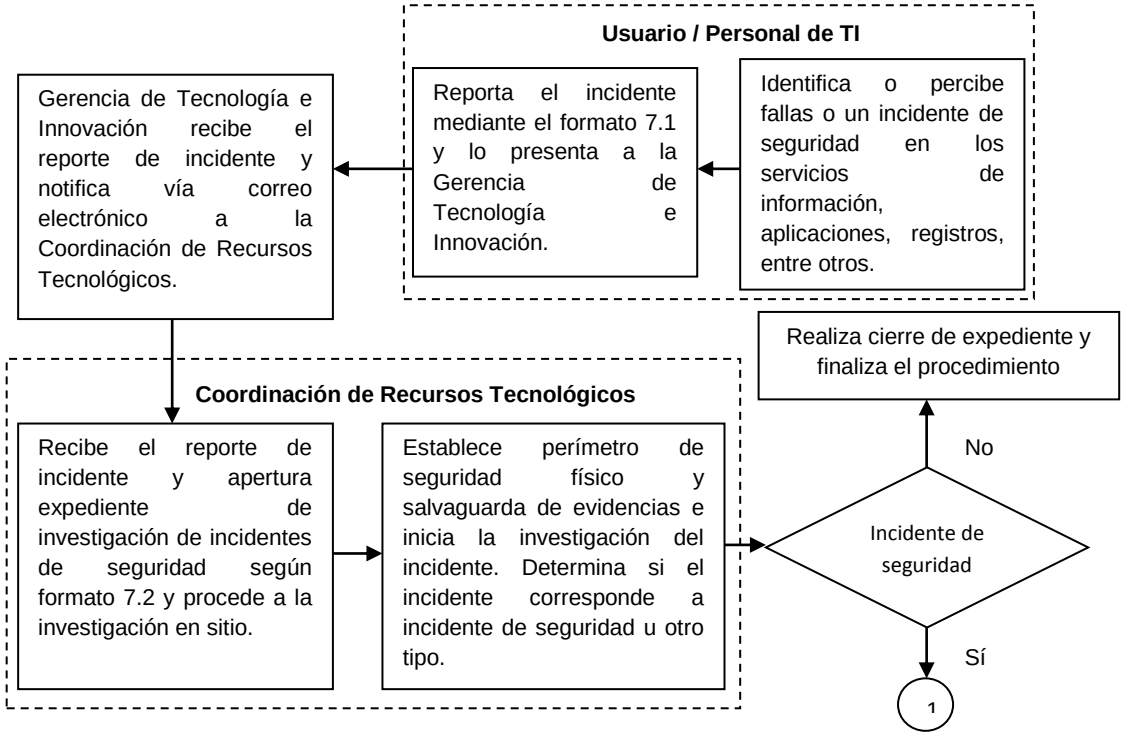
Es responsabilidad de la Gerencia de Tecnología e Innovación dar seguimiento y monitoreo al reporte de incidentes de seguridad, su investigación, resolución, valoración y documentación.

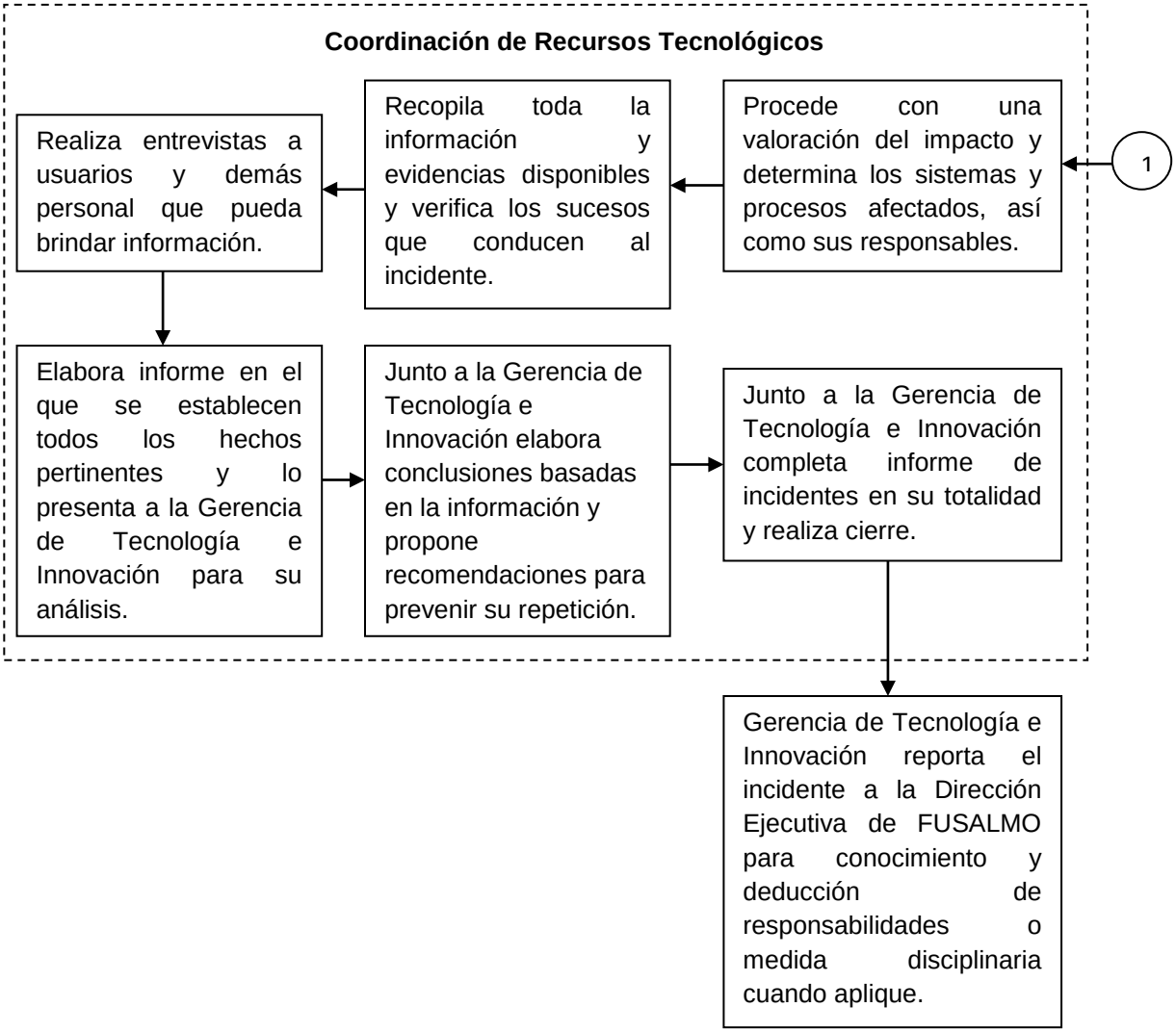
5. DESCRIPCIÓN DEL PROCEDIMIENTO DE REPORTE Y SEGUIMIENTO DE INCIDENTES DE SEGURIDAD.

No.	Responsable	Actividad
1	Usuario/ Personal de la Gerencia de Tecnología e Innovación	Identifica o percibe fallas o un incidente de seguridad en los servicios de información, aplicaciones, registros, entre otros.
2	Usuario/ Personal de la Gerencia de Tecnología e Innovación	Reporta el incidente mediante el formato 7.1 de este documento y lo presenta en forma impresa o por correo electrónico a la Gerencia de Tecnología e Innovación.
3	Gerencia de Tecnología e Innovación	Recibe el reporte de incidente y notifica vía correo electrónico a la Coordinación de Recursos Tecnológicos.
4	Coordinación de Recursos Tecnológicos	Recibe el reporte de incidente y apertura expediente de investigación de incidentes de seguridad según formato 7.2 de este documento y procede a la investigación en sitio.
5	Coordinación de Recursos Tecnológicos	Establece perímetro de seguridad físico y salvaguarda de evidencias e inicia la investigación del incidente. Determina si el incidente corresponde a incidente de seguridad u otro tipo.
6	Coordinación de Recursos Tecnológicos	Si corresponde a incidente de seguridad procede con una valoración del impacto: determina los sistemas y procesos

No.	Responsable	Actividad
		afectados, así como sus responsables.
7	Coordinación de Recursos Tecnológicos	Recopila toda la información y evidencias disponibles y verifica los sucesos que conducen al incidente.
8	Coordinación de Recursos Tecnológicos	Realiza entrevistas a usuarios y demás personal que pueda brindar información.
9	Coordinación de Recursos Tecnológicos	Elabora informe en el que se establecen todos los hechos pertinentes y lo presenta a la Gerencia de Tecnología e Innovación para su análisis.
10	Coordinación de Recursos Tecnológicos/ Gerencia de Tecnología e Innovación	Elabora conclusiones basadas en la información y propone recomendaciones para prevenir su repetición.
11	Coordinación de Recursos Tecnológicos/ Gerencia de Tecnología e Innovación	Completa informe de incidentes en su totalidad y realiza cierre.
12	Gerencia de Tecnología e Innovación	Reporta el incidente a la Dirección Ejecutiva de FUSALMO para conocimiento y deducción de responsabilidades o medida disciplinaria cuando aplique.

6. DIAGRAMA DEL PROCEDIMIENTO DE REPORTE Y SEGUIMIENTO DE INCIDENTES DE SEGURIDAD.




Coordinación de Recursos Tecnológicos
Procede con una valoración del impacto y determina los sistemas y procesos afectados, así como sus responsables.
1
Recopila toda la información y evidencias disponibles y verifica los sucesos que conducen al incidente.
Realiza entrevistas a usuarios y demás personal que pueda brindar información.
Elabora informe en el que se establecen todos los hechos pertinentes y lo presenta a la Gerencia de Tecnología e Innovación para su análisis.
Junto a la Gerencia de Tecnología e Innovación elabora conclusiones basadas en la información y propone recomendaciones para prevenir su repetición.
Junto a la Gerencia de Tecnología e Innovación completa informe de incidentes en su totalidad y realiza cierre.
Gerencia de Tecnología e Innovación reporta el incidente a la Dirección Ejecutiva de FUSALMO para conocimiento y deducción de responsabilidades o medida disciplinaria cuando aplique.

7. FORMATOS RELACIONADOS

7.1 Reporte de incidente de seguridad

REPORTE DE INCIDENTE DE SEGURIDAD	
Fecha de Notificación:	Hora de Notificación:
DATOS DE LA PERSONA QUE REPORTA EL INCIDENTE	
Nombre Completo:	
Puesto:	Área/Dependencia:
Sede:	Tel:
Correo electrónico:	
INFORMACIÓN DEL INCIDENTE	
Fecha en que se observó el incidente:	Hora en que se observó el incidente:
Descripción del incidente:	
Áreas o sistemas afectados:	

F. _____

Usuario

7.2 Expediente de investigación y reporte de incidente de seguridad

EXPEDIENTE DE INVESTIGACIÓN DE INCIDENTE DE SEGURIDAD	**CASO No.**_____
Fecha de Apertura de expediente:	Fecha de reporte del incidente:
DATOS DE LA PERSONA QUE REPORTO EL INCIDENTE	
Nombre Completo:	
Puesto:	Área/Dependencia:
Sede:	Tel:
Correo electrónico:	
INFORMACIÓN DEL RECURSO AFECTADO	
Sistema, computadora o red afectada:	
Localización física:	
Sistema Operativo u otras características:	
Seleccionar las opciones que apliquen en el análisis e investigación:	

¿Existe copia de respaldo de los datos o software afectado?	Sí		No		¿El recurso afectado tiene conexión a internet?	Sí		No	

EVIDENCIAS			
Inspección Preliminar:	**Incidente de Seguridad de la información**	Sí	No

1. Evidencias del caso
Detalle:
2. Entrevistas
Nombre de la persona entrevistada:
Resumen de Entrevista:
Nombre de la persona entrevistada:
Resumen de Entrevista:
Nombre de la persona entrevistada:
Resumen de Entrevista:

DIAGNÓSTICO			
Uso indebido de información crítica.		Uso prohibido de un recurso informático	
Divulgación no autorizada de información personal.		Eliminación insegura de información.	
Intrusión física.		Modificación o eliminación no autorizada de datos.	
Destrucción no autorizada de información.		Anomalía o vulnerabilidad técnica de software.	
Robo o pérdida de información.		Fraude o phishing.	
Interrupción prolongada en un sistema o servicio de red.		Modificación no autorizada del sitio o página web.	
Modificación, instalación o eliminación no autorizada de software.		Amenaza o acoso por medio electrónico.	
Acceso o intento de acceso no autorizado a un sistema informático.		Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.)	
Robo o pérdida de un recurso informático.		Otro:	
RESULTADOS			
RECOMENTACIONES			

F. _____

Responsable

PROCEDIMIENTO DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Preparado por	
Nombre	**Firma**
Puesto	**Fecha**

Revisado por	
Propietario	**Director (si aplica)**
Nombre **Firma**	**Nombre** **Firma**
Puesto **Fecha**	**Puesto** **Fecha**

Aprobado por	
Nombre	**Firma**
Puesto	**Fecha**

Copia controlada	
Titular	**Copia número**
El propietario del procedimiento es el responsable de la revisión anual, actualizaciones, monitoreo, control y la aprobación de este procedimiento.	

PROCEDIMIENTO DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

1. OBJETIVO

Evaluar y controlar las actividades y desempeño de los sistemas de información a fin de constatar si sus actividades son correctas y de acuerdo a los procedimientos establecidos en la Fundación.

2. ALCANCE

2.1 Inclusiones

Este procedimiento aplica para todos los sistemas que operan en FUSALMO, entre ellos correo Institucional, página web, Sistema Administrativo Financiero (SAF) y Sistema de RRHH.

2.2. Exclusiones

No se define exclusiones a este procedimiento.

3. DEFINICIONES

3.1 Plan de auditoría

Plan de trabajo anual de actividades relacionado con el proceso de auditoría, el cual es planificado, ejecutado y en seguimiento por la Gerencia de Tecnología e innovación para su desarrollo y cumplimiento. Este plan no es el programa de auditoría que ejecuta el equipo auditor.

3.2 Programa de auditoría

Planificación del trabajo en el proceso de auditoría, el cual es organizado, ejecutado y en seguimiento por el Equipo Auditor; incluye las actividades como revisiones documentales, entrevistas, reunión inicial, presentación de informe, entre otros elementos.

3.3 Informe de auditoría

Al finalizar la auditoria por parte del Equipo Auditor , se deberá generar un informe dirigido al responsable del área afectada solicitando las acciones correctivas correspondientes (si es que hubiera necesidad) y darle posterior seguimiento y cierre.

El informe contara además con una fecha específica para el cierre de los hallazgos acorde a la siguiente clasificación:

Clasificación	Descripción	Tiempo de Respuesta
Observación	Identificación de una condición potencial que puede ser la causa de incumplimiento de algún estándar o procedimiento, después de tres consecutivas observaciones del mismo tema se convertirá en una no conformidad.	5 días hábiles después de presentar el informe.
No conformidad	El no cumplimiento a un estándar, procedimiento, manual establecido el cual es documentado por la evidencia entrada por el auditor.	7 días hábiles después de presentar el informe; en caso la no conformidad sea determinando como violación se tendrá que dar respuesta de inmediato.

La respuesta al reporte enviado por el auditor debe contener lo siguiente:

- Causa Raíz: es la base de la acción a largo plazo para eliminar el problema y prevenir su repetición.
- Acción Intermedia: acción inmediata para solventar la no conformidad.
- Acción a futuro: acción a tomar para prevenir la recurrencia.

Las repuestas o plan de mejora (si aplica) son enviados por la Gerencia de Tecnología e Innovación, detallando las acciones que dan respuesta y solución a los hallazgos presentados en el informe de auditoría.

En el caso que el auditado necesita pedir extensión para dar respuesta a la no conformidad, estas serán otorgadas por el auditor si están justificadas; sin embargo el tiempo de respuesta no debe superar los 30 días calendario.

Extensiones no serán aprobadas si:

- Si la evidencia no es enviada
- Si la prórroga se solicita después de la fecha de vencimiento de la no conformidad.

3.4 Registros del Sistema de Auditorias:

Todos los registros pertenecientes a la implementación del Sistema de Auditorias de la Gerencia de Tecnología e Innovación, se encuentran archivados en la Unidad de Auditoría Interna.

Cada registro debe incluir las evidencias de las no conformidades encontradas, así como la aceptación de estos por parte del responsable.

3.5 Cierre de Auditoria

El cierre de la auditoria, se dará hasta que el auditor este satisfecho con las respuestas y evidencias del cumplimiento del plan de acción de las no conformidades presentadas por el auditado.

4. RESPONSABILIDAD

Es responsabilidad del Gerente de Tecnología e Innovación velar por el seguimiento del Plan de auditoría de la Unidad, a fin de que esta se realice en el período programado y cumpla con los requerimientos del mismo. Así también es responsable de garantizar las condiciones y disponibilidad de recursos e

información para el Equipo Auditor y la formulación y seguimiento del plan de mejora relacionado con el informe de auditoría.

Es responsabilidad de la Dirección Ejecutiva, dirigir y velar por el cumplimiento del proceso de auditoría interna, su divulgación e involucramiento de los colaboradores de la Fundación.

5. DESCRIPCIÓN DEL PROCEDIMIENTO DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN.

No.	Responsable	Actividad
1	Gerencia de Tecnología e Innovación	Planifica el plan de auditoría interna de acuerdo a las necesidades de la Fundación.
2	Gerencia de Tecnología e Innovación	Presenta a Dirección Ejecutiva el plan de auditoria y los recursos requeridos.
3	Dirección Ejecutiva	Convoca a reunión de trabajo para conformación de equipo auditor, considerando representación de las áreas críticas de la fundación; del área de TI deberá excluirse del equipo auditor.
4	Dirección Ejecutiva	Notifica a todas las áreas de la Fundación el inicio del proceso, el cronograma de desarrollo y el comité auditor. Envía notificación al área de Tecnología e innovación.
5	Gerencia de Tecnología e Innovación	Organiza las actividades en el área, coordina con equipo de trabajo, disponibilidad de documentos y demás evidencias.
6	Dirección Ejecutiva	Llegada la fecha planificada, la Dirección Ejecutiva convoca a la Gerencia de Tecnología e Innovación a reunión de presentación de los miembros del equipo auditor. Se realiza: Revisión del alcance, los objetivos, cronograma de auditoría, metodología, procedimientos a utilizar y tabla de tiempos de la auditoría.

No.	Responsable	Actividad
7	Equipo Auditor	Coordina las actividades según el plan de auditoría.
8	Equipo Auditor	Ejecuta la auditoría realizando verificación documental, demostración y entrevista respecto a los procedimientos de seguridad, controles, documentación y prácticas del área.
9	Equipo Auditor	Define acciones de mejora, hallazgo, periodos de respuesta, proceso de seguimiento, cierre de casos y referencias normativas relacionadas para la elaboración del informe de auditoría.
10	Equipo Auditor	Presenta informe de auditoría a la Dirección Ejecutiva, Gerencia de Tecnología e Innovación y demás jefaturas consideradas.
11	Gerencia de Tecnología e Innovación	Emite por escrito respuesta al informe de auditoría en relación a los hallazgos señalados, para lo cual cuenta con tres días hábiles para su preparación y evidencias.
12	Gerencia de Tecnología e Innovación	Presenta a la Dirección Ejecutiva plan de mejora a los hallazgos señalados.
13	Dirección Ejecutiva	Autoriza el plan de mejora para su ejecución.
14	Gerencia de Tecnología e Innovación	Realiza seguimiento a las acciones de mejora.

6. DIAGRAMA DEL PROCEDIMIENTO DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN.