PLAN DE IMPLEMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN - PISI

Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo - FONDESIF

CONTENIDO

1. Antecedentes. 2
2. Introducción 3
3. Fuentes Principales de Información 4
4. Términos y Definiciones 5
5. Responsabilidades y funciones 9
5.1. Responsabilidad de la Máxima Autoridad Ejecutiva (MAE) 9
5.2. Responsabilidad de Responsable de Seguridad de la Información (RSI) 9
5.3. Responsabilidad y funciones del Comité de Seguridad de la Información (CSI) 10
6. Objetivo General 11
7. Objetivos Específicos 11
8. Alcance 11
9. Metodología de gestión de Riesgo 12
10. Evaluación del Riesgo 19
11. Control de criticidad de activos de información Institucional Priorizados 23
12. Controles Mínimos de Seguridad de la Información 25
13. Indicadores y métricas 26
14. Controles por implementar 26
15. Cronograma de Implementación 27
ANEXOS 29

1. Antecedentes.

En el marco del Decreto Supremo N° 2514 se crea el Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB) fue creado el 2015, como parte de un esfuerzo por modernizar el Estado y avanzar en la implementación del Gobierno Electrónico en Bolivia, con un enfoque en la digitalización de procesos y la mejora de la eficiencia en la gestión pública.

Previamente se identificó la necesidad de modernizar las instituciones gubernamentales mediante la implementación de tecnologías de la información y comunicación (TIC) con la finalidad de mejorar la eficiencia, transparencia y participación masiva de la ciudadana en los servicios públicos.

Es así que, el Decreto Supremo estableció el CTIC-EPB como un organismo oficial encargado de coordinar la implementación de las TIC en el gobierno con el propósito de garantizar la interoperabilidad de los sistemas y promover el uso de estándares abiertos, buscando digitalizar los procesos de gestión pública de manera efectiva a través de la coordinación de estrategias conjuntas.

Desde su creación, el Consejo ha desempeñado un papel central en la elaboración de normativas, estándares, lineamientos y protocolos necesarios para la integración de las TIC en las instituciones estatales, se ha encargado de desarrollar políticas y guías que aseguren la automación de procesos que mejoren la interacción entre el Estado y los ciudadanos.

El CTIC-EPB continúa siendo un ente crucial para coordinar y guiar la transformación digital en Bolivia, facilitando una gestión pública más eficiente y accesible.

El Grupo de Trabajo de Seguridad del CTIC-EPB, planteó como objetivo la formulación de los lineamientos para que las entidades o instituciones públicas del Estado Plurinacional de Bolivia, puedan elaborar e implementar sus Planes Institucionales de Seguridad de la Información, dando como resultado un documento denominado "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público", mismo que recoge las deliberaciones, análisis y sugerencias del Grupo de Seguridad del CTIC-EPB.

En ese contexto corresponde la elaboración del Plan Institucional de Seguridad de la Información – PISI, en virtud a la necesidad de reforzar la seguridad de la información de la entidad, en respuesta a la creciente digitalización y la necesidad de proteger los datos críticos frente a amenazas cibernéticas, para:

- Protección de la infraestructura tecnológica: Con el avance de las tecnologías y la dependencia de sistemas digitales, contar con mecanismos que aseguren la integridad, confidencialidad y disponibilidad de la información.
- Cumplimiento de las normativas de seguridad y estándares internacionales, asegurando que los procedimientos de gestión de información cumplan con las leyes nacionales e internacionales sobre protección de datos.
- Estrategias para mitigar vulnerabilidades y evitar incidentes de seguridad, que podrían poner en riesgo la operación de la entidad.

El PISI tiene el objetivo de establecer un marco claro de políticas y procedimientos que guíen en la gestión de riesgos tecnológicos, implementación de controles de seguridad, y la creación de una cultura de protección de la información. Además, permitirá mejorar la respuesta ante incidentes de seguridad y fomentar una infraestructura tecnológica fortalecida y preparada a los desafíos del entorno cibernético actual.

2. Introducción

La seguridad informática se ha convertido en un componente esencial para el funcionamiento eficiente y seguro de cualquier institución. El FONDESIF como entidad generadora de información en el marco de la normativa vigente orientada al cierre tiene el reto de proteger sus activos digitales y la información sensible que maneja, en ese contexto se ha elaborado el Plan Institucional de Seguridad Informática (PISI), documento que establece las directrices, procedimientos y normativas necesarias para salvaguardar la integridad, confidencialidad y disponibilidad de la información de la entidad.

La elaboración del PISI se basa en el análisis y diagnóstico de los antecedentes institucionales y el marco normativo vigente. Entre los antecedentes se toma en cuenta los sistemas y digitalización de los procesos administrativos lo que ha incrementado la necesidad de contar con medidas fortalecidas de seguridad informática para proteger los datos y sistemas utilizados.

La Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación (Ley N° 164) y su relación intrínseca con el Plan Institucional de Seguridad de la Información (PISI), se engloba en un contexto donde las comunicaciones y el manejo de la información digital son pilares fundamentales de la sociedad y el Estado boliviano, resulta crucial comprender cómo la legislación establece el marco para el desarrollo y la regulación del sector de las telecomunicaciones y las TIC, al mismo tiempo que se articula con las estrategias de seguridad de la información para proteger los activos y garantizar la continuidad de las operaciones. Este análisis explorará la convergencia entre los mandatos de la ley de comunicaciones y los lineamientos del PISI, destacando la importancia de una gestión integral que abarque tanto el acceso y el desarrollo de las tecnologías como la protección de la información en el entorno digital boliviano.

Asimismo, el PISI se nutre de los lineamientos y mejores prácticas internacionales en materia de seguridad de la información, tales como las normas ISO/IEC 27001 y 27002, que proporcionan un marco de referencia para la gestión de la seguridad de la información y el establecimiento de controles adecuados.

En ese sentido, el Plan Institucional de Seguridad Informática pretende proporcionar un instrumento, eficiente y eficaz, para la gestión de la seguridad de la información incluyendo la identificación y evaluación de riesgos, la implementación de medidas preventivas y correctivas, y la capacitación continua al personal en materia de seguridad informática, garantizando la protección de sus activos digitales y el cumplimiento de las normativas vigente con propósito de cierre, contribuyendo así a la eficiencia y transparencia en la gestión pública.

El PISI además de ser una herramienta para la protección de la información, se constituye también en marco referencial integral y coherente, que contempla el compromiso con la seguridad, la confianza y la mejora continua en la gestión de sus procesos y servicios.

3. Fuentes Principales de Información

El Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo – FONDESIF, forma parte de las entidades bajo tuición del Ministerio de Planificación del Desarrollo – MPD, dentro la estructura organizativa del Órgano Ejecutivo del Estado Plurinacional de Bolivia.

Es una entidad pública que fue creada con la finalidad de ampliar la base patrimonial de las entidades financieras del sistema de intermediación financiera de carácter privado, constituidas como sociedades por acciones bajo la Ley de Bancos y Entidades Financieras y el Código de Comercio, en el marco del Decreto Supremo N° 24110 de fecha 1ro. de septiembre de 1995.

En la actualidad la entidad rige su accionar en el marco del Decreto Supremo N° 28999 de 1ro. de enero de 2007, que determina que el FONDESIF entrará en un proceso de disolución gradual hasta su liquidación definitiva, así también el Decreto Supremo N° 5115 de 8 de febrero de 2024, establece nuevas directrices orientadas al cierre de la entidad.

El FONDESIF en el marco de la Ley N° 777 del Sistema de Planificación Integral del Estado – SPIE de 21 de enero de 2016 y la Ley N° 1407 de 9 de noviembre de 2021 que aprueba el Plan de Desarrollo Económico y Social (PDES) 2021-2025. "Reconstruyendo la Economía para Vivir Bien, Hacia la Industrialización con Sustitución de Importaciones" contribuye a la planificación de mediano plazo a través de los siguientes planes:

- Plan Estratégico Ministerial – PEM
- Plan Estratégico Institucional - PEI

El FONDESIF cuenta con un Plan Operativo Anual – POA aprobado mediante Resolución de Consejo Superior N° 001 de 11 de septiembre de 2024, formulando las siguientes acciones de corto plazo enfocadas al cierre de la entidad.

- Asegurar los procesos necesarios que permitan la Administración y transferencia del Programa de Mecanización-PROMEC de manera óptima y operativa en el marco de la disolución del FONDESIF, según el Decreto Supremo N° 28999, con la finalidad de que los resultados continúen contribuyendo al Plan de Desarrollo Económico Social.
- Asegurar los procesos necesarios que permitan la Administración y transferencia del Programa de Mecanización-PROMEC de manera óptima y operativa en el marco de la disolución del FONDESIF, según el Decreto Supremo N° 28999, con la finalidad de que los resultados continúen contribuyendo al Plan de Desarrollo Económico Social.
- Cerrar los Fideicomisos, Programas y Proyectos inactivos, así como los que están en etapa de cierre financiero, comunicando a los involucrados en el contrato y/o convenios, según los procedimientos legales que sean pertinentes.
- Transferir la información financiera de maquinaria PROMEC, productos AGRONEGOCIOS, la Tecnología MICROFINANZAS, para que las EIFs y los beneficiarios tengan continuidad en sus operaciones.
- Administrar bienes, acciones, derechos y contingencias en el cumplimiento de las atribuciones de la Institución y en el marco de los procedimientos que regulan la materia, para contar con el cierre y transferencia de manera transparente.

En ese contexto corresponde la elaboración del Plan Institucional de Seguridad de la Información – PISI del FONDESIF que responda y se articule a la normativa vigente en el marco del cierre de la entidad, respondiendo y respetando los Lineamientos generados para ese fin.

4. Términos y Definiciones

ACTIVO: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

APLICACIONES CRÍTICAS: Son las aplicaciones o sistemas de información que reciben este término porque previamente**.**

BASE DE DATOS: Se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información.

BRECHA: Termino que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que germinen vulnerabilidades que impacten el negocio de la Entidad.

BUENAS PRÁCTICAS: Son lineamientos que contiene los principios básicos y generales para el desarrollo de los productos o servicios de la organización para la satisfacción al cliente.

CICLO DE VIDA DE LA INFORMACIÓN: Se refiere a la clasificación y almacenamiento de la información; siendo necesario tener en cuenta los requisitos técnicos y legales; así como tener claro los conceptos de disponibilidad y velocidad que depende de la misma clasificación que varía conforme su valor con el tiempo.

CLASIFICACIÓN DE LAS APLICACIONES: Las aplicaciones se clasifican conforme los procesos de la entidad.

CLASIFICACIÓN DE LA INFORMACIÓN: Proceso formal que se utiliza para ubicar el nivel a la información de la Entidad con el fin de protegerla; previa estructura de valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada. Generalmente la información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

CONTINGENCIA: Es la consecuencia de acciones o imprevistos, que puede poner en peligro la integridad, disponibilidad y confidencialidad de la información.

CORRIENTE ELECTRICA REGULADA: Se utiliza para regular o mantener el voltaje de la red eléctrica para que no afecte el funcionamiento de los recursos TIC de la Entidad.

DATO: Es una letra, número o símbolo que tiende a convertirse en información.

DEPENDENCIA: Son los grupos que conforman la estructura organizacional de la Entidad.

DISPONIBILIDAD: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieren.

DOCUMENTO: Es el medio físico que contiene la información que se quiere transmitir.

DUEÑO DE LA INFORMACIÓN: Es cualquier persona que es propietaria de la información y tiene la responsabilidad de custodiarla.

FONDESIF: Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo.

INCIDENTE: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o reducción de la calidad del servicio.

INFORMACIÓN: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas, o audiovisuales y que se guarda en cualquier medio ya sea magnético, en papel, en pantallas de computadoras, audiovisuales u otro.

INFORMACIÓN DIGITAL: Cuando la información está almacenada en un medio magnético porque cuando imprime se convierte en documento físico y en este último caso existe en el FONDESIF la dependencia que define los lineamientos, normas, guías y estándares.

INFORMACIÓN SENSIBLE: Es la tipificación que recibe la información que no es considerada de acceso público como por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más como es usar este término para designar datos privados relacionados con internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.

INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

PLAN DE CONTINGENCIAS: El plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de los servicios.

POA: Plan Operativo Anual

POLITICA TIC: Documento que contiene los lineamientos que define la organización para reglamentar el desarrollo de los proyectos y recursos TIC de la Entidad, como las acciones que deben permanecer en el tiempo para alcanzar los objetivos de su negocio.

POLITICAS DE SEGURIDAD: Es el documento de normas y lineamientos de seguridad de la información que define la Entidad para evitar que surja vulnerabilidades que puede afectar el negocio de la Entidad.

PROCESOS CRITICOS: Concepto que se utiliza para definir el conjunto de actividades o eventos que se ejecutan bajo ciertas circunstancias que inciden en los productos misionales de la entidad y en la satisfacción de los funcionarios.

PROCESAMIENTO REMOTO: Incorpora el concepto de telecomunicación, hoy día hace referencia a un dispositivo como un teléfono móvil o una computadora portátil, con capacidad de operar en red mediante comunicación inalámbrica.

PROPIETARIO DE LA INFORMACIÓN: Se utiliza para denominar a la persona autorizada para organizar, clasificar y valorar la información de su dependencia o área conforme al cargo de la estructura organizacional de la Entidad.

REPOSITORIO DE DOCUMENTOS: Sitio centralizado donde se almacena y mantiene información digital actualizada para consulta del personal autorizado.

RESPALDO DE INFORMACIÓN O COPIA DE SEGURIDAD (BACKUP): Es la copia total o parcial de información de las aplicaciones, bases de datos, archivos, documentos, configuraciones y otros, guardada en un medio de almacenamiento. Estos deben estar disponibles para su recuperación en caso de daños o accidentes.

RECUPERACIÓN: Proceso de restablecer la información de dispositivos de almacenamiento que se encuentran dañados o defectuosos.

REQUERIMIENTO: Necesidad de un servicio TIC que el usuario solicita a través del mecanismo definido por la institución en los procedimientos normalizados.

SERVICIO: Incluye los servicios profesionales para la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, enajenaciones, arrendamientos y contratación de Hardware y soporte tanto de software como de hardware; así como de la plataforma tecnológica.

SERVICIOS TIC: El concepto de Servicio TIC consiste en dar soporte, de forma integrada y personalizada, a todas estas herramientas que necesita hoy en día el profesional de empresa para realizar su trabajo. Los elementos del Servicio TIC son:

- Los dispositivos: PC, portátiles, agendas electrónicas, impresoras, teléfonos, sistemas de videoconferencia, etc.
- La Red de Área Local corporativa (LAN), Así como las comunicaciones de voz incluyendo el teléfono y ahora llega el momento de proporcionar y gestionar los PC y la electrónica de red necesarios para las comunicaciones de datos.
- Las comunicaciones de voz y datos WAN (Red de Área Remota), que incluyen tanto las redes privadas corporativas como el acceso a redes públicas como Internet. La integración de las comunicaciones WAN y estas cada vez se requieren con las comunicaciones LAN.
- Los servicios y aplicaciones desde la Red. Existe una clara tendencia hacia la "externalización" de determinados servicios de acuerdo a la madurez y sus problemas conocidos y controlados. Un ejemplo es el correo electrónico, Muchas empresas prefieren "externalizar" este servicio para no tener que dedicar recursos a mantener y gestionar la infraestructura de correo durante las 24 horas los 7 días de la semana.

SGSI: Sistema de Gestión de Seguridad de la Información. Concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización, que debe tener la política, estructura organizativa, procedimientos, procesos y recursos necesarios para implantar la gestión de la seguridad de la Información.

SISTEMA DE INFORMACIÓN: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

TIC: Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, en la actualidad no solo una

computadora hace referencia al procesamiento de la información. Internet forma parte de ese procesamiento que, quizás se realice de manera distribuida y remota.

USUARIO: Persona que utiliza los recursos TIC y que interactúen de forma activa en un proceso, secuencia, código etc.

VPN: Siglas de red privada virtual por su nombre en inglés (Virtual Prívate Network).

VULNERABILIDADES: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de la Información que pueden ser explotadas por factores externos y no controlables por la entidad (Amenazas), las cuales se constituyen en fuentes de riesgo.

5. Responsabilidades y funciones

5.1. Responsabilidad de la Máxima Autoridad Ejecutiva (MAE)

La Máxima Autoridad Ejecutiva del Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo es el ***Director General Ejecutivo***.

La Máxima Autoridad deberá:

a) Estar informada sobre el estado de Seguridad de la Información de la entidad o institución pública bajo su tutela.
b) Tomar conocimiento de la normativa vigente respecto a seguridad de la información (Decreto Supremo N° 2514 de 9 de septiembre de 2015 y Decreto Supremo N° 1793, de 13 de noviembre de 2013, de reglamentación a la Ley 164).
c) Designar al responsable de Seguridad de la Información (RSI).
d) Conformar el comité de Seguridad de la Información (CSI).
e) Asegurar que los objetivos y alcances del Plan Institucional de la Información sean compatibles con los objetivos del Plan Estratégico Institucional.
f) En lo posible, destinar los recursos administrativos, económicos y humanos para la elaboración e implementación del Plan Institucional de Seguridad de la Información.
g) Aprobar el Plan Institucional de Seguridad de la información de su entidad o institución.
h) Cumplir y hacer cumplir el Plan Institucional de Seguridad de la Información en su entidad o institución.
i) Asumir otras acciones a favor de la seguridad de la información.

5.2. Responsabilidad de Responsable de Seguridad de la Información (RSI)

El Responsable de Seguridad de la Información es el ***Encargado de Sistemas*** del Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo

El Responsable de Seguridad de la Información (RSI) será el o la profesional, con perfil y experiencia en gestión de seguridad de la información, designado por la MAE, que tendrá como función principal la elaboración e implementación del PISI.

El RSI tendrá las siguientes funciones:

a) Gestionar, elaborar e implementar el Plan Institucional de Seguridad de la Información (PISI).
b) Realizar la evaluación de riesgos de seguridad de la información en coordinación con los responsables de activos de la información.
c) Proponer la Política de Seguridad de la Información (PSI), que estará incorporada dentro del PISI.
d) Gestionar el cumplimiento del PISI.
e) Elaborar manuales de procesos y/o procedimientos de seguridad específicos que se desprenden de los lineamientos del Plan Institucional de Seguridad de la Información y promover su difusión en la entidad o institución pública.
f) Sugerir prácticas de desarrollo de software seguro para generar procesos formales que tengan presentes los controles de seguridad necesarios para la entidad o institución.
g) Coordinar la inducción, capacitación y comunicación del personal, en el marco del PISI.
h) Gestionar y coordinar la atención y respuesta a incidentes de seguridad de la información en su entidad o institución.
i) Coadyuvar en la gestión de contingencias tecnológicas.
j) Proponer estrategias y acciones en mejora de la seguridad de la información.
k) Promover la realización de auditorías al Plan Institucional de Seguridad de la información.
l) Gestionar la mejora continua de la seguridad de la información.
m) Sugerir medidas de protección ante posibles ataques informáticos que puedan poner en riesgo las operaciones normarles de la institución.
n) Realizar acciones de informática forense, en caso de ser necesario, para identificar, preservar, analizar y validar datos que puedan ser relevantes.
o) Monitorear la implementación y uso de mecanismos de seguridad, que coadyuven a la reducción de los riesgos identificados.
p) Otras funciones que resulten necesarias para preservar la seguridad de la información.

5.3. Responsabilidad y funciones del Comité de Seguridad de la Información (CSI)

El Comité de Seguridad de la Información esta con formado por:

- ***Encargado de Sistemas (RSI)***
- ***Director de Asuntos Administrativos***
- ***Director Jurídico***
- ***Profesional de Planificación***

El CSI restablecerá su organización interna y asumirá como mínimo las siguientes funciones:

a) Revisar el Plan Institucional de Seguridad de la Información (PSI).
b) Promover la aprobación del PISI a través de la MAE.

c) Revisar los manuales de procesos y/o procedimientos de seguridad que se desprenden de la Política de Seguridad de la Información incorporada en el PISI.
d) Proponer estrategias necesarias para la implementación y/o fortalecimiento de controles de seguridad en el marco de la mejora continua.
e) Realizar el seguimiento y control de los indicadores y métricas establecidos y definir las acciones que correspondan al respecto.
f) Promover la concientización y capacitación en seguridad de la información al interior de la entidad o intuición pública.
g) Proponer y promover las acciones necesarias en función a la gravedad de los incidentes de seguridad de la información, con el fin de prevenir incidentes futuros.
h) Otras funciones que resulten necesarias para la seguridad de la información.

6. Objetivo General

Realizar un diagnóstico de la situación actual en cuanto a la seguridad de información de FONDESIF y diseñar un Plan Institucional de Seguridad de la Información (PISI) que permita desarrollar operaciones seguras basadas en políticas de controles claros y conocidos por todo el personal de la Entidad.

7. Objetivos Específicos

- Identificar las vulnerabilidades desde un punto de vista operativo.
- Analizar el tratamiento de la información por parte del personal y evaluar los riesgos a partir de los procesos.
- Analizar los riesgos asociados a los activos de la información.
- Definir una gestión de riesgos de rápida respuesta para los sistemas de información.
- Gestionar el inventario de activos de información y su valoración.
- Realizar la gestión de riesgos y su valoración.
- Gestión de riesgos y sus controles.
- Gestión de controles implementados y por implementar.
- Cronograma de implementación de controles.

8. Alcance

Identificar los riesgos de los activos de información a la parte tecnológica del FONDESIF y establecer controles para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la Información relacionada.

También se describirá los lineamientos para proteger la información del FONDESIF y los recursos tecnológicos con la que se procesa y se almacena, así como la recuperación de la información mantenida a nivel de medios (discos, discos rígidos, entre otros).

Además, este documento cubre la seguridad de la información en todas las áreas de FONDESIF, incluyendo sistemas informáticos, bases de datos, archivos físicos y activos

digitales. Se establece la gestión segura de la información en las siguientes fases del cierre:

- Identificación y resguardo de activos de información.
- Control de accesos y revocación de credenciales.
- Migración o eliminación segura de datos.
- Seguimiento y verificaciones finales.
- Disposición de equipos tecnológicos.

9. Metodología de gestión de Riesgo

El PISI contempla la gestión de riesgos en el ámbito de la seguridad de la información. Para esto, se adopta la metodología de gestión de riesgos propuesta dentro de los "*Lineamentos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público*", con el objetivo de implementar controles de seguridad o mejorar la eficacia de los controles ya existentes.

La evaluación del riesgo permitirá identificar las debilidades en cuanto a controles de seguridad inexistentes o ineficaces, además de determinar y categorizar las amenazas potenciales y vulnerabilidades asociadas a activos de información.

El resultado de este proceso permitirá determinar la identificación de controles que reducirán los riesgos.

Identificación, Clasificación y Valoración de Activos de Información.

El RSI, de forma conjunta con los responsables de los procesos identificados dentro del alcance del Plan Institucional de Seguridad de la Información, coordinó el proceso de identificación, clasificación y valoración de activos de información, haciendo uso de la guía incluida en el Anexo B de los Lineamentos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.

La identificación determina qué activos de información formarán parte del PISI haciendo uso de una clasificación.

La valoración de activos de información tiene como objetivo asegurar que la información asociada a los mismos reciba niveles de protección adecuados.

Se valorará los activos de la información en las dimensiones que requiere la institución (Disponibilidad, Integridad y Confidencialidad).

La valoración presenta una escala para la valoración cuantitativa de las características del activo de información.

A continuación, se detalla la matriz de Inventario de Activos de Información y sus respectivas valoraciones de cada activo.

MATRIZ DE INVENTARIO Y VALORACIÓN

ENTIDAD: FONDESIF

FECHA DE ELABORACIÓN 25/03/2025

FECHA DE APROBACIÓN:

INVENTARIO DE ACTIVOS IDENTIFICADOS							VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	GESTIÓN	
Nº	**ACTIVO**	**DESCRIPCIÓN**	**TIPO**	**UBICACIÓN**	**UNIDAD RESPONSABLE**	**CUSTODIO**	**DISPONIBILIDAD**	**INTEGRIDAD**	**CONFIDENCIALIDAD**		**FECHA INGRESO**	**FECHA SALIDA**
[HW] EQUIAMIENTO INFORMÁTICO (HARDWARE)												
1	Servidores Físicos	POWER EDGE R210 II TAG COLOR NEGRO POWER EDGE R7300 TAG COLOR NEGRO	EQUIPAMIENTO INFORMATICO	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Muy Alto	Medio	Medio	Alto	2010	---
2	Servidor Físico	POWER EDGE R350 COLOR NEGRO	EQUIPAMIENTO INFORMATICO	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Muy Alto	Medio	Medio	Alto		---
3	Equipo de computación de sobremesa	Computadora de escritorio para personal	EQUIPAMIENTO INFORMÁTICO	Oficina Central	Direcciones de la Entidad	Usuarios de la Entidad	Alto	Medio	Medio	Medio	2010	---
4	Equipo de computación portátil	Computadora portátil para personal	EQUIPAMIENTO INFORMÁTICO	Oficina Central	Direcciones de la Entidad	Usuarios de la Entidad	Alto	Medio	Medio	Medio	2013	---
[SW] SOFTWARE - APLICACIONES INFORMÁTICAS												
1	Servidor Virtual (correo.fondesif.gob.bo)	VMWARE - Correo Institucional	SOFTWARE - APLICACIONES INFORMATICOS	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Alto	Alto	2016	---
2	Servidor Virtual (wayra.fondesif.gob.bo)	PROXMOX- Sistema de pasajes y viáticos	SOFTWARE - APLICACIONES INFORMATICOS	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Alto	Alto	2024	
3	Active Directory	Administración de usuarios	SOFTWARE - APLICACIONES INFORMÁTICOS	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Alto	Alto	2017	---
4	DNS	Sistema de Nombre de Dominio	SOFTWARE - APLICACIONES INFORMÁTICOS	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Alto	Alto	2017	---

5	app.fondesif.gob.bo (khunu - tdfond - yanapiri)	Sistema de Créditos y Cartera Sistema correspondencia Sistema de pasajes y viáticos	SOFTWARE - APLICACIONES INFORMÁTICOS	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Alto	Alto	2017	---
6	Página Web	CMS Drupal	SOFTWARE - APLICACIONES INFORMÁTICOS	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Bajo	Medio	2010	---
7	SIF	Sistema Integrado Financiero	SOFTWARE - APLICACIONES INFORMÁTICOS	Sistemas de Información	Dirección de Asuntos Administrativos	Encargado de Sistemas	Medio	Alto	Medio	Medio	2018	---
8	VSIAF	Sistema de Activos Fijos	SOFTWARE - APLICACIONES INFORMÁTICOS	Sistemas de Información	Dirección de Asuntos Administrativos	Encargado de Sistemas	Medio	Alto	Medio	Medio	2017	---
9	Antivirus	Software Bitdefender con licencia corporativa para protección de virus	SOFTWARE - APLICACIONES INFORMATICOS	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Alto	Alto	2016	---
[S] SERVICIOS												
1	Correo Electrónico	postfix, dovecot.	SERVICIOS	Servidor Físico (correo.fondesif.gob.bo)	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Alto	Medio	2017	---
2	Active Directory	Directorio Activo (LDAP)	SERVICIOS	Servidor Físico (ad.fondesif.gob.bo)	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Medio	Alto	2017	---
3	Servidor web	Apache2, php5, java, tomcat7	SERVICIOS	Servidor Físico (www.fondesif.gob.bo)	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Alto	Alto	2016	---
4	Base de datos	Postgres, Msql, Sql Server	SERVICIOS	Servidor (bbdd-server.fondesif.gob.bo)	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Alto	Alto	2016	---
5	Servidor DNS	DNS en Windows Server	SERVICIOS	Servidor Físico (dns.fondesif.gob.bo)	Dirección de Asuntos Administrativos	Encargado de Sistemas	Muy Alto	Alto	Alto	Alto	2017	---
[COM] REDES DE COMUNICACIONES												
1	Firewall - router	Pfsense	REDES DE COMUNICACIONES	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Muy Alto	Muy Alto	Medio	Alto	2016	---

2	Router	Microtik (FIBRA OPTICA - MEGALINK)	REDES DE COMUNICACIONES	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Medio	Alto	Muy Alto	Alto	2018	---
3	Switch	Switch CISCO administrable	REDES DE COMUNICACIONES	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Muy Alto	Alto	Alto	2018	---
4	Modem	Modem VDSL - AXS	REDES DE COMUNICACIONES	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Alto	Medio	Alto	2017	---
5	Red Telefónica IP	Red Telefónica IP	REDES DE COMUNICACIONES	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Muy Alto	Alto	Medio	Alto	2010	---
6	Red LAN	Red LAN	REDES DE COMUNICACIONES	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Muy Alto	Alto	Medio	Alto	2018	---
7	NVR	Grabador de Cámaras de Seguridad	REDES DE COMUNICACIONES	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Medio	Alto	Alto	Alto	2010	---
[D] DATOS INFORMACIÓN												
1	Documentos contables 1995 - 2019	Preventivos (ingreso, diario, egresos y ajustes)	INFORMACIÓN	Of. Deposito C/ Rosendo Gutiérrez Edif. Multicentro	Dirección de Asuntos Administrativos	Encargado de Archivo	Alto	Medio	Medio	Medio	2019	---
2	Documentos de correspondencia interna y externa 1995 - 2015	Cartas recibidas enviadas, instructivos, memorándum resoluciones)	INFORMACIÓN	Of. Deposito C/ Rosendo Gutiérrez Edif. Multicentro	Dirección General	Encargado de Archivo	Alto	Medio	Medio	Medio	2015	---
3	Documentos de proyectos 2005 - 2021	Programas fonadal. yungas y paps	INFORMACIÓN	Of. Deposito C/ Rosendo Gutiérrez Edif. Multicentro	Dirección de Asuntos Administrativos	Encargado de Archivo	Medio	Medio	Medio	Medio	2021	---
4	Documentos del personal 1996 - 2021	Hojas de vida	INFORMACIÓN	Of. Deposito C/ Rosendo Gutiérrez Edif. Multicentro	Dirección de Asuntos Administrativos	Encargado de Archivo	Alto	Medio	Medio	Medio	2021	---
5	Documentos legales 1997 - 2019	Resoluciones, convenios, contratos e informes	INFORMACIÓN	Of. Deposito C/ Rosendo Gutiérrez Edif. Multicentro	Dirección Jurídica	Encargado de Archivo	Medio	Medio	Medio	Medio	2019	---

6	Carpetas de Procesos de Contratación 2004 - 2020	Documentación relacionada a los procesos de contrataciones que realiza la entidad en la gestión vigente y la anterior	INFORMACION	Of. Deposito C/ Rosendo Gutiérrez Edif. Multicentro	Dirección de Asuntos Administrativos	Encargado de Archivo	Alto	Bajo	Medio	Medio	2020	---
7	Documentación (Aportes patronales y Aportes AFP) 2003 - 2019	Aportes patronales y AFP del personal que trabaja en la entidad	INFORMACIÓN	Oficina de Recursos Humanos y Servicios	Dirección de Asuntos Administrativos	Encargado de Archivo	Alto	Alto	Medio	Alto	2019	---
8	Correspondencia Interna (Hojas de Ruta) 1999 - 2015	Hojas de ruta interna y externa que se generan en la entidad	INFORMACIÓN	Oficina de Recursos Humanos y Servicios	Dirección de Asuntos Administrativos	Encargado de Archivo	Alto	Alto	Medio	Alto	2015	---
9	Formúlanos 110 de personal dependiente 1999 - 2020	Formularios 110 de personal de la entidad y reportes de Impuestos internos	INFORMACIÓN	Oficina de Recursos Humanos y Servicios	Dirección de Asuntos Administrativos	Encargado de Archivo	Medio	Bajo	Medio	Medio	2020	---
10	Contratos de Personal y Bienes y Servicios	Información desde gestiones 2013-2018	INFORMACIÓN	Oficina Jurídica	Dirección Jurídica	Director Jurídico	Alto	Alto	Medio	Alto		---
11	Convenios Interinstitucional e Inter gubernativo	Convenios Interinstitucional e Inter gubernativo	INFORMACIÓN	Oficina Jurídica	Dirección Jurídica	Director Jurídico	Alto	Alto	Medio	Alto		---
12	Memoriales	Memoriales	INFORMACIÓN	Oficina Jurídica	Dirección Jurídica	Director Jurídico	Alto	Alto	Medio	Alto		---
13	Fotocopia de procesos Judiciales 1989 - 2015	Fotocopia de procesos Judiciales	INFORMACIÓN	Oficina Jurídica	Dirección Jurídica	Director Jurídico	Alto	Medio	Medio	Alto	2015	---
14	Actas de Transferencias	Actas de Transferencias	INFORMACIÓN	Oficina Jurídica	Dirección Jurídica	Director Jurídico	Alto	Alto	Medio	Alto	2020	---
15	Testimonios	Testimonios	INFORMACIÓN	Oficina Jurídica	Dirección Jurídica	Director Jurídico	Alto	Alto	Medio	Alto		---
16	Gacetas Oficiales 1995 - 2005	Gacetas Oficiales	INFORMACIÓN	Oficina Jurídica	Dirección Jurídica	Director Jurídico	Medio	Bajo	Medio	Medio	2005	---
17	Publicaciones (Revistas, boletines, trípticos. Bipticos entre otros)	Publicaciones (Revistas, boletines, trípticos. Bipticos entre otros)	INFORMACIÓN	Oficina de Visibilidad	Dirección General	Encargado de Archivo	Medio	Medio	Bajo	Medio		---
[MEDIA] SOPORTE DE INFORMACIÓN												
1	Material digital (Videos, Cuñas Radiales y artes) Formato físico y digital	Material digital (Videos, Cuñas radiales y artes)	SOPORTE DE INFORMACIÓN	Oficina de Visibilidad	Dirección General	Secretaria Ejecutiva	Alto	Medio	Bajo	Medio	2020	---
[AUX] EQUIPAMIENTO AUXILIAR												
1	UPS	Sistema de alimentación ininterrumpida	EQUIPAMIENTO AUXILIAR	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Muy Alto	Modio	Bajo	Medio	2019	---

2	Aire Acondicionado	Aire Acondicionado en CPD	EQUIPAMIENTO AUXILIAR	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Muy Alto	Medio	Bajo	Medio	2021	---
3	Cableado Estructurado	Cableado estructurado	EQUIPAMIENTO AUXILIAR	Data Center	Dirección de Asuntos Administrativos	Encargado de Sistemas	Alto	Medio	Bajo	Medio	2015	---
[L] INSTALACIONES												
1	Instalaciones	Lugar donde se hospedan los sistemas de información y comunicación	EQUIPAMIENTO AUXILIAR	Data Center	Unidad de Planificación	Encargado de Sistemas	Muy Alto	Alto	Muy Bajo	Medio	2010	---

10. Evaluación del Riesgo

El responsable del activo de información determina; en base a sucesos y la importancia que tiene el activo sobre las posibles amenazas y vulnerabilidades a las que se está expuesto y realiza una descripción del escenario en el cual se puede dar la materialización de la amenaza, asumiendo que el responsable conoce y entiende los riesgos sobre el activo de la entidad o institución pública.

Una vulnerabilidad es toda aquella debilidad que presenta el activo de información, dada comúnmente por la inexistencia o ineficacia de un control.

Una amenaza es todo elemento que haciendo uso o aprovechando una vulnerabilidad, atenta o puede atentar contra la seguridad de un activo de información. Las amenazas surgen a partir de la existencia de vulnerabilidades, independientemente de que se comprometa o no la seguridad de un sistema.

La Evaluación del Riesgo es la metodología seleccionada que realiza la identificación, análisis y valoración de los riesgos asociados a los activos de información previamente identificados, clasificados y valorados y permite identificar amenazas y vulnerabilidades.

Para la identificación del Riesgo se toma en cuenta las vulnerabilidades y amenazas que inciden en la confidencialidad, integridad y disponibilidad de la información.

Análisis y Valoración del Riesgo evalúa las posibles consecuencias de la materialización de una amenaza producto de las vulnerabilidades presentes en los activos de información.

La priorización está claramente establecida a partir del nivel de riesgo máximo definido previamente por la entidad o institución pública a través del CSI.

		PROBABILIDAD				
		Improbable	**Poco probable**	**Probable**	**Muy Probable**	**Cierta/ Inminente**
IMPACTO	**Irrelevante**	Irrelevante	Irrelevante	Irrelevante	Bajo	Bajo
	Menor	Irrelevante	Bajo	Bajo	Medio	Medio
	Moderado	Irrelevante	Bajo	Medio	Alto	Alto
	Severo	Bajo	Medio	Alto	Alto	Crítico
	Crítico	Bajo	Medio	Alto	Crítico	Crítico

Matriz de Valoración de Riesgo

MATRIZ DE VALORACIÓN DEL RIESGO

ENTIDAD: FONDESIF

FECHA DE ELABORACIÓN 7/4/2025

FECHA DE APROBACIÓN:

VALORACIÓN DEL RIESGO							
Nº	**ACTIVO**	**AMENAZA**	**SITUACIÓN**	**VULNERABILIDAD**	**PROBABILIDAD**	**IMPACTO**	**NIVEL DE RIESGO**
[HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)							
1	Servidores Físicos	Condiciones ambientales adversas	Falla física de los servidores	Sensibilidad a la humedad, polvo, suciedad	Probable	Severo	Alto
		Falla del hardware	Falla de equipo por ausencia de mantenimientos preventivos	Mantenimiento deficiente	Probable	Severo	Alto
2	Equipo de computación de sobremesa	Acceso indebido por usuarios internos o externos	Falta de control en actualización de contraseñas	Ausencia de un eficiente control de cambios en la configuración.	Poco Probable	Severo	Medio
		Error de mantenimiento / actualización de programas software y hardware	Mala configuración en el equipo para actualizar el equipo	Configuración incorrecta de parámetros, Ausencia de control de cambios en la configuración.	Poco Probable	Severo	Medio
3	Equipo de computación portátil	Acceso indebido por usuarios internos o externos	Falta de control en actualización de contraseñas	Ausencia de un eficiente control de cambios en la configuración.	Poco Probable	Severo	Medio
		Error de mantenimiento / actualización de programas software y hardware	Mala configuración en el equipo para actualizar el equipo	Configuración incorrecta de parámetros, Ausencia de control de cambios en la configuración.	Poco Probable	Severo	Medio
[SW] SOFTWARE - APLICACIONES INFORMÁTICAS							
1	Servidor Virtual (correo.fondesif.gob.bo)	Acceso no autorizado desde otras máquinas virtuales	Intento de ingreso de personas ajenas a la entidad	Falta de segmentación entre entornos virtuales	Poco Probable	Severo	Medio
2	Servidor Virtual (wayra.fondesif.gob.bo)	Acceso no autorizado desde otras máquinas virtuales	Intento de ingreso de personas ajenas a la entidad	Falta de segmentación entre entornos virtuales	Poco Probable	Severo	Medio
3	khuno.fondesif.gob.bo	Perdida de Información	Error en el sistema causa pérdida de información	Carencia de archivos de respaldo para información sensible	Probable	Severo	Alto

4	tdfond.fondesif.gob.bo	Perdida de Información	Error en el sistema causa pérdida de información	Carencia de archivos de respaldo para información sensible	Probable	Severo	Alto
5	Active Directory	Acceso no autorizado a objetos del dominio	Usuario obtiene permisos administrativos sin autorización	Ausencia de documentación actualizada. Configuración incorrecta de parámetros.	Poco Probable	Moderado	Bajo
6	DNS	Ataques de redirección	Atacante modifica la resolución de nombres	Mala configuración del servidor	Poco Probable	Moderado	Bajo
7	App.fondesif.gob.bo	Perdida de Información	Error en el sistema causa pérdida de información	Carencia de archivos de respaldo para información sensible	Poco Probable	Severo	Medio
8	Pagina Web	Falsificación de solicitud entre sitios	Usuario mal intencionado envía datos	Gestión débil de sesiones y autenticación	Probable	Moderado	Bajo
9	SIF	Perdida de Información	Error en el sistema causa pérdida de información	Carencia de archivos de respaldo para información sensible	Probable	Moderado	Bajo
10	VSIAF	Perdida de Información	Error en el sistema causa pérdida de información	Carencia de archivos de respaldo para información sensible	Poco Probable	Moderado	Bajo
11	Antivirus	Manipulación de la configuración	Usuario mal intencionado podría modificar la configuración	Configuración incorrecta de parámetros	Poco Probable	Moderado	Bajo
[S] SERVICIOS							
1	Correo electrónico	Malware a través de archivos adjuntos	Falta de control de correos maliciosos	Falta de filtros antispam/antimalware	Poco Probable	Severo	Medio
2	Active Directory	Escalada de privilegios	Usuario obtiene permisos administrativos sin autorización	Usuarios con privilegios excesivos	Poco Probable	Moderado	Bajo
3	Servidor web	Acceso no autorizado	Falta de control en actualización de contraseñas	Deficiente gestión de Inexistente contraseñas	Probable	Severo	Alto
4	Base de datos	Acceso no autorizado a datos sensibles	Falta de control en actualización de contraseñas	Permisos mal configurados	Poco Probable	Severo	Medio
5	Servidor DNS	Ataques de redirección	Mala configuración	Mala configuración del servidor	Poco Probable	Moderado	Bajo
[COM] REDES DE COMUNICACIONES							

1	Firewall - router	Ataques por configuración incorrecta	Falla de configuración	Falta de registro de registros	Poco Probable	Severo	Medio
2	Router	Intercepción del tráfico	Mala configuración en el equipo	Puertos abiertos innecesarios	Poco Probable	Moderado	Bajo
3	Switch	Intercepción del tráfico	Mala configuración en el equipo	Puertos abiertos innecesarios	Poco Probable	Moderado	Bajo
4	Red Telefónica IP	Intercepción de llamadas	Llamadas expuestas	Tráfico sin cifrado	Probable	Moderado	Bajo
5	Red LAN	Difusión de software dañino	Mala configuración en el equipo o control regular del equipo	Segmentación de red Inexistente	Poco Probable	Moderado	Bajo
[D] DATOS INFORMACIÓN							
1	Documentos Físicos	Divulgación	Falta de control en la clasificación de Documentos	Copias no controladas de documentos confidenciales	Probable	Severo	Alto
		Pérdida de Información	Ausencia de capacitación al personal sobre la seguridad de la información	Fallas de medio de almacenamiento	Probable	Severo	Alto
[AUX] EQUIPAMIENTO AUXILIAR							
1	UPS	Corte de suministro eléctrico	Corre peligro que el equipo no funcione por falta de energía eléctrica	Ausencia de cambio de baterías	Poco Probable	Moderado	Bajo

11. Control de criticidad de activos de información Institucional Priorizados

Activo:	Archivos Físicos
Tipo:	Datos de Información
Riesgo Actual:	Critico

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual			Control Recomendado	Actividad
			Probabilidad	Impacto	Nivel Riesgo		
Acceso no autorizado	La falta de procedimientos y herramientas para la clasificación y protección de la información	Usuarios y contraseñas	Muy probable	Crítico	Crítico	3.2.3. Revisión, eliminación o ajuste de los derechos de acceso	Acción de clasificación de información
Divulgación	Copias no controladas de documentos confidenciales	Inexistente	Muy probable	Crítico	Crítico	2.3.2. Eliminación segura de la información	Acción para la protección y resguardo de información clasificada
Pérdida de Información	Fallas de medio de almacenamiento	Se cuenta con back up actualizado	Muy probable	Moderado	Alto	6.2.1. Respaldos de Información	Capacitación al personal de la entidad respecto a seguridad de información

Activo:	Servidores
Tipo:	Hardware - Equipamiento Informático
Riesgo Actual:	ALTO

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual			Control Recomendado	Actividad
			Probabilidad	Impacto	Nivel Riesgo		
Condiciones ambientales adversas	Sensibilidad a la humedad, polvo, suciedad	Se cuenta con un CPD	Muy probable	Moderado	Alto	5.3.1. Condiciones operativas	Adaptación del Ambiente
Suministro de energía y equipos de continuidad eléctrica	Sensibilidad a variaciones de tensión / Fuente de alimentación Inestable	Componente de energía UPS	Muy probable	Crítico	Crítico	5.3.1. Condiciones operativas	Mantenimiento de UPS
Falla del hardware	Mantenimiento deficiente	Se realiza Mantenimiento correctivo	Muy probable	Moderado	Alto	6.2.1. Respaldos de Información	Mantenimiento Correspondiente
Acceso no autorizado	Actualización del ingreso biométrico	Se cuenta con control biométrico	Poco Probable	Moderado	Alto	5.1.2. Trabajo en áreas e instalaciones seguras	Acción para la actualización del control biométrico

Activo:	Sistemas - TDFOND / KHUNU
Tipo:	Software - Aplicaciones Informáticas
Riesgo Actual:	ALTO

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual			Control Recomendado	Actividad
			Probabilidad	Impacto	Nivel Riesgo		

Acceso no autorizado	Carencia de procedimientos para el acceso a sistemas de información	Usuarios y contraseñas	Muy probable	Crítico	Crítico	3.2.3. Revisión, eliminación o ajuste de los derechos de acceso	Acción para el control de altas, bajas y modificación de los derechos de acceso y cambio de contraseña
Perdida de Información	Carencia de archivos de respaldo para información sensible	Inexistente	Muy probable	Crítico	Crítico	3.2.2. Responsabilidad de los usuarios para la autentificación	Acción para la gestión de Backups
Monitoreo de tráfico	No se cuenta con un programa de análisis de vulnerabilidad	Inexistente	Muy probable	Crítico	Crítico	6.1.3. Gestión de la capacidad	Acción para el análisis y gestión de vulnerabilidades técnicas
Cyber amenazas	Carencia de requerimientos de seguridad	Inexistente	Muy probable	Crítico	Crítico	3.2.2. Responsabilidad de los usuarios para la autentificación	Acción para contingencias tecnológicas

12. Controles Mínimos de Seguridad de la Información

Los controles de Seguridad de la información que serán implementados se encuentran referenciados en “Controles Implementados y por Implementar”.

13. Indicadores y métricas

Los indicadores y métricas empleados al momento de identificar criticidades, así como elaborar y desarrollar el control de seguridad de nuestro Plan de Seguridad de la Información, serán aplicadas también a tiempo de evaluar a eficacia de los controles implementados en los activos priorizados.

Se necesita métricas vinculadas a los objetivos de seguridad y los procesos necesarios específicos. Los indicadores aplicados a la valoración inicial, que serán aplicados — a su vez — para medir la reducción de la criticidad en los activos priorizados, se encuentran inmersos en:

- Identificar los Activos de Información.
- Realizar un análisis de riesgo bajo una metodología de riesgos, identificando los riesgos y amenazas en cada uno de los activos de información.
- Identificar el nivel de seguridad existente en los sistemas, servicios, aplicaciones e infraestructura (incidentes, actualizaciones)
- Definir y planificar los planes de acción a realizar (corto, mediano y largo plazo)
- Implementar mecanismos de seguridad, con los siguientes controles:

  1. Gestión de activos de la información
  2. Control de accesos
  3. Seguridad física y ambiental
  4. Seguridad de las operaciones

Las métricas utilizadas consistirán en medidas definidas y adaptadas, tanto a nivel estratégico (progreso del cronograma) como táctico y operativo (procesos y controles de la Política de seguridad de la información). En cada nivel las métricas deben tener las propiedades de ser:

a) Especifico

b) Medible cualitativa a cuantitativamente y/o con indicadores y atributos.

c) Alcanzable.

d) Relevante.

e) Repetible en periodos de tiempo.

14. Controles por implementar

LISTA DE CONTROLES IMPLEMENTADOS Y POR IMPLEMENTAR		
Control	**Si / No**	**Justificación**
2.3.2. Eliminación segura de la información	**SI**	
3.2.1. Administración de accesos, cancelación y privilegios de usuario	**SI**	
3.2.3. Revisión, eliminación o ajuste de los derechos de acceso	**SI**	

6.2.1. Respaldos de Información	**SI**	
5.1.2. Trabajo en áreas e instalaciones segura	**SI**	
5.3.1. Condiciones operativas	**SI**	
6.2.1. Respaldos de Información	**SI**	
3.2.2. Responsabilidad de los usurarios para la autentificación	**SI**	
3.2.3. Revisión, eliminación o ajuste de los derechos de acceso	**SI**	
6.1.3. Gestión de la capacidad	**SI**	
6.1.3. Gestión de la capacidad	**SI**	

15. Cronograma de Implementación

En el marco del Plan Institucional de Seguridad de la Información, la entidad o institución pública elabora un cronograma de implementación de los controles definidos. Para esto, todos los procesos y/o procedimientos que se desprenden de la Política de Seguridad de la Información ya se encuentran elaborados para su aplicación.

Los controles implementados serán validados y/o actualizados.

El cronograma de implementación contempla mínimamente:

CRONOGRAMA DE IMPLEMENTACIÓN							
Nº	**ACTIVO DE INFORMCIÓN PERSONALIZADO**	**CONTROLES A IMPLEMENTARSE**	**ACCIONES A DESARROLLAR**	**FECHA INICIO**	**FECHA CONCLUSIÓN**	**RESPONASBLES**	**REQUERIMIENTO PARA LA IMPLEMENTACIÓN DE LA ACCIÓN**
1	Archivos Físicos	2.3.2. Eliminación segura de la información 3.2.1. Administración de accesos, cancelación y privilegios de usuario 3.2.3. Revisión, eliminación o ajuste de los derechos de acceso 6.2.1. Respaldos de Información	1. Acción de clasificación de información. 2. Acción para la protección y resguardo de información clasificada. 3. Capacitación al personal de la entidad respecto a seguridad de información	1/5/2025	1/5/2026	• Personal de Sistemas eventual y/o Consultor • RSI	Capacitación al personal de la entidad respecto a la Seguridad de la Información
3	Servidores	5.1.2. Trabajo en áreas e instalaciones segura 5.3.1. Condiciones operativas 6.2.1. Respaldos de Información	1. Acción para el control de cambio de contraseñas 2. Adaptación del Ambiente 3. Mantenimiento Correspondiente	1/5/2025	1/5/2026	• Personal de Sistemas eventual y/o Consultor • RSI	Capacitación al personal de la entidad respecto a la Seguridad de la Información

3	Sistemas	3.2.2. Responsabilidad de los usuarios para la autentificación 3.2.3. Revisión, eliminación o ajuste de los derechos de acceso 6.1.3. Gestión de la capacidad	1. Acción para contingencias tecnológicas 2. Acción para el control de altas, bajas y modificación de los derechos de acceso y cambio de contraseña 3. Acción para la gestión de Backups 4. Acción para el análisis y gestión de vulnerabilidades técnicas	1/5/2025	1/5/2026	• Personal de Sistemas eventual y/o Consultor • RSI	Capacitación al personal de la entidad respecto a la Seguridad de la Información

ANEXOS