RESOLUCIÓN ADMINISTRATIVA Nro. 392/2023
La Paz, 27 de noviembre de 2023

CONSIDERANDO:

Que la Constitución Política del Estado Plurinacional de 07 de febrero de 2009, en el Parágrafo II del Artículo 103 del Texto Constitucional, señala que el Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.

Que la Ley Nro. 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación de 8 de agosto de 2011 en su Artículo 71, declara de prioridad nacional la promoción del uso de las tecnologías de información y comunicación para procurar el vivir bien de todas las bolivianas y bolivianos.

Que el Parágrafo I del Artículo 75 de la citada Ley, dispone que el nivel central del Estado promueve la incorporación del Gobierno Electrónico a los procedimientos gubernamentales, a la prestación de sus servicios y a la difusión de información, mediante una estrategia enfocada al servicio de la población.

Que el Artículo 76 de la precitada Ley, establece que el Estado fijará los mecanismos y condiciones que las Entidades Públicas aplicarán para garantizar el máximo aprovechamiento de las tecnologías de la información y comunicación, que permitan lograr la prestación de servicios eficientes; asimismo, el Parágrafo I del Artículo 77 de la referida Ley, señala que los Órganos Ejecutivo, Legislativo, Judicial y Electoral en todos sus niveles, promoverán y priorizarán la utilización del software libre y estándares abiertos, en el marco de la soberanía y seguridad nacional.

Que la Ley Nro. 650 de 15 de enero de 2015, eleva a rango de Ley la "Agenda Patriótica del Bicentenario 2025", misma que determina como Pilar 4 "Soberanía científica y tecnológica con identidad propia" y Pilar 11 "Soberanía y transparencia en la gestión pública bajo los principios del no robar, no mentir y no ser flojo".

Que el Decreto Supremo Nro. 2514 de 9 de septiembre del 2015, crea la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC como una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica, y patrimonio propio, bajo tuición del Ministerio de la Presidencia.

Que el inciso i) del Artículo 7 de la normativa señalada establece que la AGETIC tiene como función elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática.

Que el inciso b) del Artículo 8 del citado Decreto Supremo, prevé que, el Centro de Gestión de Incidentes Informáticos, como parte de la estructura técnico operativa de la AGETIC, tiene la función d establecer los lineamientos para la elaboración de Planes Institucionales de Seguridad de la Información de las entidades del sector público.

Que el parágrafo II del Artículo 17 del referido Decreto, prescribe que las entidades del sector público deberán desarrollar el plan institucional de Seguridad de la Información acorde a los lineamientos establecidos por el Centro de Gestión de Incidentes Informáticos.

Que mediante Resolución Administrativa AGETIC/RA/0051/2017, modificada por la Resolución Administrativa AGETIC/RA/0059/2018, se aprueban los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del sector público.

Que el Numeral 5 de los citados lineamientos define el Plan Institucional de Seguridad de la Información (PISI), como el documento que establece las actividades relativas a la organización y gestión de la seguridad de la información en la entidad o institución pública.

Que el inciso g) del Numeral 6.1.1. de los señalados lineamientos dispone que, es deber de la Máxima Autoridad Ejecutiva aprobar el Plan Institucional de Seguridad de la Información de su entidad o institución.

Calle Belisario Salinas Nro. 573, entre Presbítero Medina y Andrés Muñoz • Sopocachi
Teléfono: (591-2) 2128276 • Fax: (591-2) 2128299 / La Paz • Bolivia
www.fdi.gob.bo
@FDIBolivia

RESOLUCIÓN ADMINISTRATIVA Nro. 392/2023
La Paz, 27 de noviembre de 2023

Que el inciso a) del Numeral 6.1.2 de los referidos lineamientos, establece como función del Responsable de la Seguridad de Información gestionar, elaborar e implementar el Plan Institucional de Seguridad de la Información.

Que mediante Decreto Supremo Nro. 2493 de 26 de agosto de 2015, dispone en el Artículo 2 que: "I. Se crea el Fondo de Desarrollo Indígena como Institución Pública Descentralizada con personalidad jurídica y patrimonio propio, así como autonomía de gestión, administrativa, financiera, legal y técnica, bajo tuición del Ministerio de Desarrollo Rural y Tierras"; "III. El Fondo de Desarrollo Indígena está a cargo de un Director General Ejecutivo, el cual deberá ser designado mediante Resolución Suprema y no cuenta con Directorio".

Que mediante Resolución Suprema Nro. 27381 de 23 de diciembre de 2020, se designa a la ciudadana a la Lic. Delicia Rossio López Tolaba, con C.I. No. 1890689 Tarija, como Directora General Ejecutiva del Fondo de Desarrollo Indígena – FDI.

Que la Resolución Administrativa Nro. 342/2023 de 10 de noviembre de 2023 que modifica la Resolución Administrativa Nro. 043/2023 de 6 de febrero de 2023 mediante la cual se conforma el Comité de Seguridad de la Información (CSI) y Designa a los Responsables de Seguridad de la Información (RSI) del Fondo de Desarrollo Indigena, establece en su parte Dispositiva Segunda que: "Se mantiene firme y subsistente la designación de los demás integrantes del Comité de Seguridad de la Información (CSI) y así como de los Responsables de Seguridad de la Información (RSI), del Fondo de Desarrollo Indígena, bajo el siguiente detalle actualizado: Delicia Rossio Lopez Tolaba, Directora General Ejecutiva del Fondo de Desarrollo Indígena, en su calidad de Presidenta del Comité de Seguridad de la Información – CSI. (con posibilidad de delegar funciones); Ronald Guarachi Asistiri, Asesor de Despacho del Fondo de Desarrollo Indígena, en su calidad de Miembro del Comité de Seguridad de la Información – CSI; Ángel Álvarez Candia, Jefe del Departamento de Asuntos Jurídicos y Gestión Legal de Proyectos del Fondo de Desarrollo Indígena, en su calidad de Miembro del Comité de Seguridad de la Información – CSI; Wilber Arancibia Aymuro, Jefe del Departamento Administrativo Financiero del Fondo de Desarrollo Indígena, en su calidad de Miembro del Comité de Seguridad de la Información – CSI; Sabino Carbasuyo Ríos, Jefe del Departamento Técnico de Proyectos del Fondo de Desarrollo Indígena, en su calidad de Miembro del Comité de Seguridad de la Información – CSI; Omar Hugo Paz Gómez, Responsable del Área de Planificación del Fondo de Desarrollo Indígena, en su calidad de Miembro del Comité de Seguridad de la Información – CSI; José Luis Carpio Bravo, Responsable de Administración y Personal del Fondo de Desarrollo Indígena, en su calidad de Miembro del Comité de Seguridad de la Información – CSI; José Luis Quispe Layme, Profesional en Seguridad de la Información y Software Libre del Fondo de Desarrollo Indígena, en su calidad de Responsable de Seguridad de la Información - RSI y Secretario del Comité de Seguridad de la Información – CSI y Félix Nina Cruz, Profesional de Sistemas Informáticos del Fondo de Desarrollo Indígena, en su calidad de Responsable de Seguridad de la Información – RSI.

Que el Comité de Seguridad de la Información del Fondo de Desarrollo Indigena en fecha 27 de noviembre de la presente gestión, aprobó por unanimidad de sus miembros el "Plan Institucional de Seguridad de la Información" y la "Política de Seguridad de la Información", disponiendo su correspondiente remisión a la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación – AGETIC.

Que El Área de Sistemas Informáticos dependiente del Departamento Administrativo Financiero mediante Informe INF/FDI/DAF/AAyP/SIS/0186-23 de 27 de noviembre de 2023, remite a la Máxima Autoridad Ejecutiva el Plan Institucionas de Seguridad de la Información (PISI) y Políticas de Seguridad de la Información (PSI) del Fondo de Desarrollo Indigena para su revisión y aprobación mediante Resolución Administrativa, asimismo concluye y recomienda que: "El Plan Institucional de Seguridad de la Información (PISI) versión 1.0 y la Política de Seguridad de la Información (PSI) versión 1.0 del Fondo de Desarrollo Indígena son documentos que establecen las directrices, objetivos, controles para garantizar la confidencialidad, la integridad y la disponibilidad de la información institucional. El PISI se ha elaborado siguiendo los lineamientos normativos vigentes y realizando diversas actividades, como la evaluación de riesgos, la elaboración del PSI y el cronograma de implementación. El PISI representa un avance importante para la gestión y la protección de la información del FDI, pero también implica un compromiso y una responsabilidad de todos los actores involucrados. Por ello, se recomienda su difusión, su capacitación, su implementación y su seguimiento, para asegurar su efectividad y su mejora continua. Se remite el documento final de la Plan Institucional de Seguridad de la Información (PISI) versión 1.0 y Política de Seguridad de la

Calle Belisario Salinas Nro. 573, entre Presbítero Medina y Andrés Muñoz • Sopocachi
Teléfono: (591-2) 2128276 • Fax: (591-2) 2128299 / La Paz • Bolivia
www.fdi.gob.bo
@FDIBolivia

RESOLUCIÓN ADMINISTRATIVA Nro. 392/2023
La Paz, 27 de noviembre de 2023

Información (PSI) versión 1.0 que es parte del mismo para su revisión y aprobación mediante Resolución Administrativa".

Que el Departamento de Asuntos Jurídicos y Gestión Legal de Proyectos emite el Informe Legal CITE: INF-FDI-DAJyGLP-Nro. 0977-2023 de 27 de noviembre de 2023, en el cual concluye que: "(...) la solicitud de aprobación del Plan Institucional de Seguridad de la Información (PISI) versión 1.0 y Política de Seguridad de la Información (PSI) versión 1.0 que es parte del mismo, se encuentra debidamente justificado mediante el informe INF/FDI/DAF/AAyP/SIS/0186-23 emitido por la Unidad de Sistemas dependiente del Departamento Administrativo Financiero del FDI, por lo que es viable su aprobación mediante una Resolución Administrativa de conformidad a lo establecido en el inciso g), numeral 6.1.1 de la Resolución Administrativa AGETIC/RA/0051/2017, modificada por la Resolución Administrativa AGETIC/RA/0059/2018, que aprueba los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del sector público, y las atribuciones del Fondo de Desarrollo Indígena, establecidas en el Decreto Supremo Nro. 2493 de 26 de agosto de 2015"; asimismo recomienda: "(...) a la Máxima Autoridad Ejecutiva del FDI suscribir la Resolución Administrativa que aprueba el Plan Institucional de Seguridad de la Información (PISI) versión 1.0 del Fondo de Desarrollo Indígena y la Política de Seguridad de la Información (PSI) versión 1.0 que es parte del mismo, adjunto por el Área de Sistemas dependiente del Departamento Administrativo Financiero de conformidad al Informe INF/FDI/DAF/AAyP/SIS/ 0186-23 de 30 de noviembre de 2023, que en anexo formara parte integrante e indivisible de la Resolución Administrativa de aprobación".

POR TANTO:

La Directora General Ejecutiva del Fondo de Desarrollo Indígena Lic. Delicia Rossio López Tolaba, en merito a las atribuciones conferidas por el Decreto Supremo No. 2493 de 26 de agosto de 2015 y demás disposiciones legales conexas. 3

RESUELVE:

PRIMERO. - Aprobar el PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI) VERSIÓN 1.0 DEL FONDO DE DESARROLLO INDIGENA, y la Política de Seguridad de la Información (PSI) Versión 1.0 que es parte del mismo, que en anexo forman parte integrante e indivisible de la presente Resolución Administrativa.

SEGUNDO. – Aprobar el Informe CITE: INF/FDI/DAF/AAyP/SIS/0186-23 de 27 de noviembre de 2023 y el Informe Legal CITE: INF-FDI-DAJyGLP-Nro. 0977-2023 de 27 de noviembre de 2023, elaborados por las áreas respectivas del Fondo de Desarrollo Indigena, que sustentan técnica y legalmente la presente Resolución Administrativa.

TERCERO. - El Departamento Administrativo Financiero del Fondo de Desarrollo Indigena a través de su unidad pertinente, queda encargado del cumplimiento de la presente Resolución Administrativa.

REGÍSTRESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.

ASESOR DE DESPACHO V°B° RGA FDI

Lic. Delicia Rossio Lopez Tolaba
DIRECTORA GENERAL EJECUTIVA
FONDO DE DESARROLLO INDIGENA
MDRyT

V°B° A.G.C.V.

V°B° G.A.

Angel Alvarez Candia
JEFE DEL DEPARTAMENTO DE ASUNTOS JURIDICOS Y GESTION LEGAL DE PROYECTOS

Calle Belisario Salinas Nro. 573, entre Presbítero Medina y Andrés Muñoz • Sopocachi
Teléfono: (591-2) 2128276 • Fax: (591-2) 2128299 / La Paz • Bolivia
www.fdi.gob.bo
@FDIBolivia

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI) DEL FONDO DE DESARROLLO INDÍGENA - FDI

GESTIÓN 2023

INFORMACIÓN GENERAL		
Nombre del documento:	Política de Seguridad de la Información	
Código:	FDI/SIS/PSI/2023	
Versión:	1.0	
CONTROL DE VERSIONES		
Versión	**Fecha**	**Descripción**
1.0	27/11/2023	Política de Seguridad de la Información
ELABORADO POR:		
Nombre	**Sello**	**Firma**
José Luis Quispe Layme	Lic. José Luis Quispe Layme PROFESIONAL EN SEGURIDAD DE LA INFORMACIÓN Y SOFTWARE LIBRE FONDO DE DESARROLLO INDÍGENA - FDI	
Félix Nina Cruz	Lic. Felix Nina Cruz PROF. DE SISTEMAS INFORMATICOS FONDO DE DESARROLLO INDIGENA - FDI	

1. INTRODUCCIÓN

El Fondo de Desarrollo Indígena – FDI tiene como misión, gestionar, financiar, ejecutar de manera directa y fiscalizar programas y proyectos para el desarrollo productivo de los pueblos indígena originarios campesinos y comunidades interculturales y afrobolivianas, en el territorio nacional.

El FDI, en su visión, se constituye en el instrumento económico por la soberanía de los pueblos indígena originarios campesinos y comunidades interculturales y afrobolivianos, que promueve e impulsa el fortalecimiento de la economía comunitaria en todos los municipios y territorios de las autonomías indígena originaria campesinas del Estado Plurinacional de Bolivia, realizando esfuerzos conjuntos de manera efectiva con las Entidades Territoriales Autónomas y las del Nivel Central del Estado.

La información es un activo valioso y estratégico para el cumplimiento de la misión y la visión del Fondo de Desarrollo Indígena – FDI. Por tal motivo, el FDI, reconoce la necesidad de proteger la información que genera, recibe, procesa, almacena y transmite, tanto en formato digital como físico, ante amenazas que pudieran afectar su confidencialidad, integridad y disponibilidad.

La presente política establece directrices de seguridad de la información en el FDI, así como definir los roles y responsabilidades de los servidores públicos involucrados en el uso y manejo de la información para la protección de la información institucional.

La política de seguridad de la información se aplica a toda la información que el FDI posee o administra, así como a los recursos tecnológicos, humanos y físicos que la soportan. La política se revisará y actualizará periódicamente, de acuerdo con los cambios en el entorno interno y externo del FDI, y con el fin de introducir un ciclo de mejora continua y sostenible en el tiempo. El FDI se compromete a implementar y mantener los controles de seguridad necesarios para garantizar la protección de la información, así como a difundir y hacer cumplir la política entre todos los servidores públicos.

2. MARCO NORMATIVO

La presente Política de Seguridad de la Información, tiene como marco normativo las siguientes disposiciones:

a) Ley Nro. 164 de 8 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación.
b) Decreto Supremo Nro. 1793 de 13 de noviembre de 2013, que aprueba el Reglamento a la Ley Nro. 164, para el Desarrollo de Tecnologías de Información y Comunicación.
c) Decreto Supremo Nro. 3527 de fecha 11 de abril de 2018, que modifica parcialmente el Decreto Supremo Nro. 1793.
d) Decreto Supremo Nro. 2514 de 9 de septiembre de 2015.
e) Decreto Supremo Nro. 3251 de 11 de julio de 2017.

f) Resolución Administrativa Nº AGETIC/RA/0051/2017 de 19 de septiembre de 2017, mediante el cual, la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, aprobó el documento "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público".

3. TÉRMINOS Y DEFINICIONES

Activo de información. Conocimientos o datos que tienen valor para la organización.

Acuerdo de confidencialidad. Documento en el cual el servidor público y/o terceros se comprometen a respetar la confidencialidad de la información y a usarla solo para el fin que se estipule.

Seguridad de la información. La seguridad de la información es la 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.

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

Disponibilidad. Propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran.

Integridad. Propiedad que salvaguarda la exactitud y completitud de la información.

Comité de Seguridad de la Información (CSI). Equipo de trabajo conformado para gestionar, promover e impulsar iniciativas en seguridad de la información.

Servidor público. Persona individual, que independientemente de su jerarquía y calidad, presta servicios en relación de dependencia a una entidad, u otras personas que presten servicios en relación de dependencia, cualquiera sea la fuente de su remuneración.

Responsable de Seguridad de la Información (RSI). Servidor público que tiene asignadas las funciones de desarrollar e implementar el Plan Institucional de Seguridad de la Información, que entre las responsabilidades está la de gestionar incidentes.

Custodio del activo de información. Servidor público encargado de administrar y hacer efectivo los controles de seguridad definidos por el responsable del activo de información.

Responsable del activo de información. Servidor público de nivel jerárquico que tiene la responsabilidad y atribución de establecer los requisitos de seguridad y la clasificación de la información vinculada al activo enmarcado al proceso del cual es responsable.

Amenaza. Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en una organización.

Riesgo. Combinación de la probabilidad de un evento adverso y su consecuencia.

Vulnerabilidad. Debilidad de un activo o control, que puede ser explotada por una amenaza.

Impacto. Cambio adverso en la operación normal de un proceso de la institución pública.

Evento de seguridad de la información. Ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información o la falla de controles o una situación previamente desconocida, que pueda ser relevante para la seguridad.

Incidente de seguridad de la información. Evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

4. OBJETIVOS

4.1. Objetivo general

Establecer directrices para proteger la información del Fondo de Desarrollo Indígena, preservando su confidencialidad, disponibilidad e integridad, en un nivel aceptable y en un marco de gestión de riesgos alineado a la estrategia de la Institución.

4.2. Objetivos específicos

a) Establecer directrices de Gestión de Activos de Información, para la identificación, valoración, clasificación y tratamiento de los activos de información que el FDI valora y tiene bajo su responsabilidad.
b) Establecer directrices para la Implementación de Controles de Seguridad de la Información, según las necesidades de la Institución y la Normativa Gubernamental sobre seguridad de la información.
c) Establecer directrices de Gestión de Incidentes de Seguridad de la Información, para identificar y minimizar los impactos adversos de los incidentes en las operaciones del FDI, mediante la implementación o mejora de controles.
d) Establecer directrices de Concientización y Capacitación en Seguridad de la Información, para que el personal del FDI conozca los controles de seguridad la información y sea responsables de prevenir incidentes.

e) Establecer directrices que expresen la posición institucional en materia de seguridad de la información, para que el personal del FDI actúe conforme a lo establecido en la política al manejar la información.

5. ALCANCE

Es de aplicación y cumplimiento obligatorio por parte de los servidores públicos, consultores individuales de línea y proveedores de servicios del Fondo de Desarrollo Indígena.

6. ROLES Y RESPONSABILIDADES

Todos los servidores o servidoras públicas de planta, eventual y consultores individuales de línea del Fondo de Desarrollo Indígena tienen la responsabilidad de asegurar la confidencialidad, integridad, y disponibilidad de la información que custodian. Además de esta responsabilidad general, las instancias responsables y los roles que ejercen para la seguridad de la información del FDI, son:

6.1. Máxima Autoridad Ejecutiva (MAE)

i. Estar informada sobre el estado de seguridad de la información de la entidad o institución pública bajo su tutela.
ii. 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).
iii. Designar al Responsable de Seguridad de la Información (RSI).
iv. Conformar el Comité de Seguridad de la Información (CSI).
v. Asegurar que los objetivos y alcances del Plan Institucional de Seguridad de la Información sean compatibles con los objetivos del Plan Estratégico Institucional.
vi. En lo posible, destinar los recursos administrativos, económicos y humanos para la elaboración e implementación del Plan Institucional de Seguridad de la Información.
vii. Aprobar la normativa interna de seguridad la información en base a las propuestas presentadas por el Responsable de Seguridad de la Información.
viii. Cumplir y hacer cumplir la normativa interna y externa relacionada a la Seguridad de la Información.
ix. Asumir otras acciones a favor de la seguridad de la información.

6.2. Responsable de Seguridad de la Información

i. Gestionar, elaborar e implementar el Plan Institucional de Seguridad de la Información (PISI).
ii. Realizar la evaluación de riesgos de seguridad de la información en coordinación con los responsables de activos de información.
iii. Proponer la Política de Seguridad de la Información, que estará incorporada dentro del PISI.
iv. Gestionar el cumplimiento del PISI.
v. Elaborar manuales de procesos y/o procedimientos de seguridad específicos que se desprendan de los lineamientos del Plan Institucional de Seguridad de la Información y promover su difusión en la entidad o institución pública.
vi. Sugerir prácticas de desarrollo de software seguro para generar procesos formales que tengan presentes los controles de seguridad necesarios para la entidad o institución.
vii. Coordinar la inducción, capacitación y comunicación del personal, en el marco del PISI.
viii. Gestionar y coordinar la atención y respuesta a incidentes de seguridad de la información en su entidad o institución.
ix. Coadyuvar en la gestión de contingencias tecnológicas.
x. Proponer estrategias y acciones en mejora de la seguridad de la información.
xi. Promover la realización de auditorías al Plan Institucional de Seguridad de la Información.
xii. Gestionar la mejora continua de la seguridad de la información.
xiii. Sugerir medidas de protección ante posibles ataques informáticos que puedan poner en riesgo las operaciones normales de la Institución.
xiv. Realizar acciones de informática forense, en caso de ser necesario, para identificar, preservar, analizar y validar datos que puedan ser relevantes.
xv. Monitorear la implementación y uso de mecanismos de seguridad, que coadyuven a la reducción de los riesgos identificados.
xvi. Otras funciones que resulten necesarias para preservar la seguridad de la información.

6.3. Comité de Seguridad de la Información

i. Revisar el Plan Institucional de Seguridad de la Información (PISI).
ii. Promover la aprobación del PISI a través de la MAE.
iii. Revisar los manuales de procesos y/o procedimientos de seguridad que se desprendan de la Política de Seguridad de la Información incorporada en el PISI.
iv. Proponer estrategias necesarias para la implementación y/o fortalecimiento de controles de seguridad en el marco de la mejora continua.
v. Realizar el seguimiento y control de los indicadores y métricas establecidos y definir las acciones que correspondan al respecto.
vi. Promover la concientización y capacitación en seguridad de la información al interior de la entidad o institución pública.
vii. 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.
viii. Otras funciones que resulten necesarias para la seguridad de la información.

6.4. Responsable del Activo de Información

i. Son responsables o propietarios de los activos de información, los Jefes de Departamento y Responsables de Área.
ii. Clasificar la información que está bajo su responsabilidad.
iii. Supervisar, controlar y promover el cumplimiento de la Política de Seguridad de la Información y la normativa interna que se desprenda de la misma, en la Unidad Organizacional a su cargo.
iv. Dar a conocer al Responsable de Seguridad de la Información del FDI, todo evento o incidente que afecte a la seguridad de la información.

6.5. Servidores Públicos (Incluye al Personal Eventual y Consultores de Línea)

i. Tomar conocimiento y dar estricto cumplimiento de la Política de Seguridad de la Información y la normativa interna que se desprenda de la misma.
ii. Dar a conocer al Responsable de Seguridad de la Información y a su inmediato superior, cualquier tipo de situación que comprometa o afecte a los sistemas y activos de información, que origine una vulneración a la seguridad o genere incumplimiento a la normativa de seguridad.

7. DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

7.1. Ámbito de seguridad: Seguridad en recursos humanos

Descripción: La seguridad en recursos humanos se refiere a establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y la entidad o institución pública con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral.

Postura institucional:

i. Todo servidor público o personal eventual o consultor de línea que se incorpore al FDI, deberá suscribir un Acuerdo de Confidencialidad, responsabilizándose de la seguridad de la información y de las sanciones correspondientes en caso de incumplimiento.
ii. Todo servidor público o personal eventual o consultor de línea del FDI, deberá participar en los eventos de concientización y capacitaciones sobre seguridad de la información que se organicen periódicamente.
iii. Todo servidor público o personal eventual o consultor de línea del FDI, ante su desvinculación y cambio de cargo, deberá devolver los activos de información bajo su custodia.
iv. Todo servidor público o personal eventual o consultor de línea que se incorpore al FDI, deberá tomar conocimiento de la Normativa Interna de Seguridad de la Información.

7.2. Ámbito de seguridad: Gestión de activos de información

Descripción: La gestión de activos de información, con el fin de preservar la integridad, disponibilidad y confidencialidad de los activos de información, se debe administrar, controlar y asignar responsabilidades en el uso y protección de los mismos.

Postura institucional:

i. La información que se genera o se recibe en cualquier etapa de su ciclo de vida, desde su creación, procesamiento, almacenamiento, transmisión, eliminación o destrucción, es propiedad del FDI y únicamente debe ser utilizada con fines institucionales.
ii. La información física generada o recibida es debidamente custodiada en Archivo Central y su acceso es controlado.
iii. Los Activos de Información del FDI son inventariados, identificando para cada uno de los mismos a su responsable y custodio, para evaluar los controles de seguridad adecuados para cada activo en base a una evaluación de riesgos.
iv. La información institucional es clasificada, etiquetada y protegida de acuerdo con su valor e importancia, establecida por los responsables de los activos de información.
v. La información institucional que no haya sido clasificada en cuanto a su confidencialidad como "pública", no deberá quedar disponible a personas o entidades externas al FDI, salvo en las situaciones y formas expresamente establecidas en la legislación y normas vigentes y con controles que garanticen su protección.
vi. El FDI debe garantizar la eliminación segura de la información que ya no sea necesaria o que haya cumplido su ciclo de vida, de acuerdo a los niveles de clasificación definidos por el mismo y normativa legal vigente, y respetando marco normativo relacionado con la retención y el resguardo de la información.
vii. La información clasificada como confidencial o reservada es transportada de manera segura, para que únicamente el destinatario autorizado tenga el acceso correspondiente, manteniendo un registro del tipo de medio, custodio y acceso.

7.3. Ámbito de seguridad: Seguridad física y ambiental

Descripción: La seguridad física y ambiental se refiere a asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica para la entidad o institución pública, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.

Postura institucional:

i. El FDI, establece áreas físicas como críticas, restringidas o controladas para la implementación de controles de seguridad que prevengan el acceso, divulgación, modificación de la información a personas no autorizadas.

ii. El FDI, monitorea la seguridad física a través de un Sistema de Video Vigilancia, con cámaras de seguridad ubicadas en los ingresos de cada ambiente.
iii. Las personas externas que ingresan a los ambientes del FDI, deberán portar la identificación de visitante en lugar visible, personal de seguridad física impedirá el acceso a las instalaciones de personas no autorizadas o que no tengan relación con las operaciones de la institución.
iv. Todos los servidores públicos portarán la credencial de identificación en un lugar visible.
v. Los servidores públicos no podrán ingresar o retirar elementos que comprometan la seguridad de la información, permitiendo realizar la inspección correspondiente al personal de seguridad física.
vi. El FDI, realizará simulacros de evacuación y respuesta ante amenazas internas, externas, ambientales y/o conflictos sociales, al menos una vez al año.
vii. Las áreas de almacenamiento de archivo, deberán contar con mecanismos de seguridad, como el control de acceso, cámara de seguridad y otros relativos a la protección de medios de almacenamiento físico para minimizar el impacto ocasionado por condiciones ambientales, incendios, inundaciones, polvo, vibraciones entre otros.
viii. Todos los servidores públicos deberán resguardar bajo llave u otro mecanismo de control, toda la información en medio de almacenamiento físico o digital a su cargo, al finalizar la jornada laboral.

7.4. Ámbito de seguridad: Gestión de incidentes de seguridad de la información

Descripción: La gestión de incidentes de seguridad de la información se refiere a establecer mecanismos para la gestión de incidentes en seguridad de la información dentro de la institución o entidad pública para dar continuidad a las operaciones y mejorar los controles de seguridad implementados.

Postura institucional:

i. Todo servidor público o personal eventual o consultor de línea del FDI, deberá velar por la seguridad de la información y comunicará al Responsable de Seguridad de la Información cualquier evento o incidente que pudiera afectar la confidencialidad, integridad y disponibilidad de la información, a través de los canales de comunicación establecidos.

7.5. Ámbito de seguridad: Cumplimiento

Descripción: El cumplimiento se refiere a asegurar el cumplimiento operativo del Plan Institucional de Seguridad de la Información que conlleva la Política de Seguridad y la documentación resultante de la misma.

Postura institucional:

i. El Responsable de Seguridad de la Información informa a la Máxima Autoridad Ejecutiva y al Comité de Seguridad de la Información, respecto al estado de cumplimiento de los controles de seguridad implementados.

8. DIFUSIÓN

El Responsable de Seguridad de la Información del FDI se encargará de difundir la Política de Seguridad de la Información a todo el personal del FDI, mediante Comunicado, al menos una vez al año. Esta difusión tendrá como base la aplicación de la Política y las disposiciones legales vigentes.

9. CUMPLIMIENTO

Todos los servidores públicos de la institución deben conocer y dar estricto cumplimiento a las directrices establecidas en la presente Política y la normativa de seguridad que se desprenda de la misma.

10. SANCIONES

El incumplimiento a lo establecido en la presente Política, según el impacto generado al FDI, será sancionado de acuerdo al régimen disciplinario del Reglamento Interno de Personal y/o a lo establecido en el Reglamento de Responsabilidad por la Función Pública aprobado por Decreto Supremo Nº 23318 –A, modificado por el Decreto Supremo Nº 26237, sin prejuicio de aplicar las sanciones legales pertinentes.