DOCUMENTO ELECTRONICO

APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA SUBSECRETARÍA DE DESARROLLO REGIONAL Y ADMINISTRATIVO, EN EL MARCO DEL SISTEMA DE MEJORA DE LA GESTIÓN Y DEJA SIN EFECTO LA RESOLUCIÓN EXENTA N° 8.328, DEL AÑO 2018, DE ESTA SUBSECRETARÍA. (E23401/2022)
RESOLUCION EXENTO Nº: 11876/2022
Santiago, 30/11/2022

VISTOS:
Lo dispuesto en la Ley N° 18.359, de 1984, que crea el cargo de Subsecretario de Desarrollo Regional y Administrativo; en el D.F.L. Nº 1-18.359, de 1985, del Ministerio del Interior, que traspasa y asigna funciones a la Subsecretaría de Desarrollo Regional y Administrativo; en el Decreto Supremo Nº 77, de 2004, y el Decreto Supremo Nº 83, de 2004, ambos del Ministerio Secretaría General de la Presidencia; en el Decreto Supremo N°258, del 09 de septiembre de 2022, que nombra al Subsecretario de Desarrollo Regional y Administrativo, y en las Resoluciones N°s. 7, de 2019 y 16, de 2020, de la Contraloría General de la República, que establecen normas sobre exención del trámite de toma de razón.

CONSIDERANDO:
1.- Que SUBDERE requiere un Sistema de Gestión de Seguridad de la Información (SGSI) que tiene por objetivo lograr niveles adecuados de integridad, confidencialidad y disponibilidad de los activos de información institucional considerados relevantes, de manera tal que se asegure la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios, funcionarios y beneficiarios de SUBDERE.

2.- Que, la Subsecretaría de Desarrollo Regional y Administrativo del Ministerio del Interior y Seguridad Pública, requiere actualizar su Política de Seguridad de la Información.

3.- Que, el presente acto administrativo viene en formalizar la actualización antes indicada.

RESUELVO:

Artículo 1º**.-** Apruébase la actualización de la Política General de Seguridad de la Información de la Subsecretaría de Desarrollo Regional y Administrativo del Ministerio del Interior y Seguridad Pública, que se establece seguidamente:

POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. DECLARACIÓN INSTITUCIONAL

La Subsecretaría de Desarrollo Regional y Administrativo (SUBDERE) tiene, por mandato legal, las funciones de coordinar, impulsar y evaluar el desarrollo regional. A la vez, debe colaborar en las funciones de modernización y reforma administrativa del Estado.

Es en este sentido que la SUBDERE considera que los activos de información son esenciales para el desarrollo de sus procesos, comprometiéndose a iniciar y sentar las bases para el desarrollo progresivo de un Sistema de Gestión de Seguridad de la Información, que asegure preservar la confidencialidad, integridad y disponibilidad de estos activos.

Lo anterior, con la finalidad de asegurar la continuidad de la seguridad de la información, dar cumplimiento a la normativa aplicable y a las definiciones estratégicas vigentes, mediante la implementación de un conjunto adecuado de medidas, que permitan gestionar los riesgos y garantizar la seguridad de la información, así como el mejoramiento continuo del sistema y el desarrollo de una cultura de seguridad institucional.

Asimismo, la SUBDERE asume el compromiso en torno a la gestión de los activos de información relevantes, a objeto de asegurar la satisfacción de las partes interesadas. Para ello, la Institución ha decidido utilizar y guiarse por la normativa señalada en apartado “4. DOCUMENTOS DE REFERENCIA”, asegurando su consistencia con el Sistema Integrado de Gestión (SIG).

Finalmente, la Autoridad del servicio reconoce la importancia y el valor de los activos de información como un elemento crítico al proceso de toma de decisiones para el cumplimiento de su Misión Institucional y, por tanto, establece la Política General de Seguridad de la Información.

2. OBJETIVOS DE LA POLÍTICA

2.1 Objetivo General de la Política: El propósito de esta política es definir la, dirección, principios y reglas básicas para la gestión de la seguridad de la información en la Subsecretaría de Desarrollo Regional y Administrativo.
2.2 Objetivos específicos:
a) Definir e implementar un conjunto de políticas, instructivos y controles orientados a garantizar la confidencialidad, integridad y disponibilidad de todo activo de información que sea responsabilidad de la Institución.
b) Definir e implementar un sistema de seguridad de la información que permita una gestión adecuada sobre el control, monitoreo y evaluación periódica de los puntos críticos en el resguardo de los activos de información, mediante un enfoque de de gestión de riesgos.

c) Contar con una estructura organizacional de soporte al Sistema de Gestión Seguridad de la Información (SGSI), que entregue lineamientos y directrices para su adecuada gestión y mejora continua.
d) Establecer un marco de responsabilidades, deberes y niveles de protección de la información, bajo el concepto de activo de información, que rijan el comportamiento de todas las personas funcionarias de planta o contrata de esta Subsecretaría, así como del personal contratado a honorarios y de terceros que presten servicios a esta Institución.
e) Asegurar el conocimiento y acceso, a través de los medios con que cuente la Institución, a la Política General de Seguridad de la Información y sus instrumentos asociados, de manera comprensible y pertinente a la labor de todas las personas involucradas en el sistema.
f) Ejecutar, aplicar e implementar medidas acordes a las directrices gubernamentales en materia de ciberseguridad.

3. ALCANCE DE LA POLÍTICA

La Política General de Seguridad de la Información se aplica a todo el personal que se desempeña en la SUBDERE, cualquiera sea su condición jurídica laboral, personas naturales y a las entidades externas que tengan acceso a los activos de información de la SUBDERE, para cuyo efecto deberán suscribirse los acuerdos correspondientes.

Además, aplica a todos los procesos de la SUBDERE, los cuales se incorporarán en forma gradual al Sistema de Gestión de Seguridad de la Información (SGSI), conforme a las prioridades que establezca el Comité de Seguridad de la Información de la SUBDERE, incluyendo a las unidades responsables del desarrollo de sus actividades y los recursos utilizados, salvo en aquellos casos en que explícitamente se indique lo contrario.

4. DOCUMENTOS DE REFERENCIA

· Decreto Supremo Nº83, de 2004, del Ministerio Secretaría General de la Presidencia, Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
· DFL 29 Fija texto refundido, coordinado y sistematizado de la ley N°18.834.
· Ley Nº21.180, de 2019, del Ministerio Secretaría General de la Presidencia, Transformación Digital del Estado.
· Normas NCh-ISO 27001 y 27002 en sus versiones vigentes.
· Política Nacional de Ciberseguridad.
· Instructivo Presidencial Nº008 del 23 de octubre de 2018, que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los Órganos de la Administración del Estado.
· Resolución vigente que Aprueba Política de Sistema Integrado de Gestión de la SUBDERE.

5. DEFINICIONES

· Sistema de Gestión de Seguridad de la Información (SGSI): Sistema que forma parte del Sistema Integrado de Gestión (SIG). Está basado en un enfoque hacia los riesgos de una institución, y su fin es establecer, implementar, operar, monitorear, mantener, evaluar y mejorar la seguridad de la información. Este sistema considera la estructura organizacional, políticas, actividades de planificación, responsabilidad, prácticas, procedimientos y recursos.
· Sistema Integrado de Gestión (SIG): Sistema que vela por los aspectos estratégicos de Calidad, Gestión de Riesgos, Seguridad de la Información y Ciberseguridad, entre otros, y su fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la gestión con el fin de satisfacer los requisitos de las partes interesadas.
· Seguridad de la Información: Es el nivel de certeza y confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Se busca proteger el recurso o activo de información de una amplia gama de amenazas, asegurando la continuidad de las operaciones de la Subsecretaría, minimizando el daño y cumpliendo su misión y objetivos estratégicos.
· Seguridad Informática: Conjunto de métodos, procesos o técnicas, para la protección de activos informáticos (redes e infraestructura) y la información digital.
· Ciberseguridad: Es la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.
· Activo de Información: Aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información, y de valor para la Institución. Se distinguen 3 niveles básicos de activos de información:
§ La Información propiamente tal, en sus múltiples formatos, a modo de ejemplo, papel, digital, texto, imagen, audio, video.
§ Los Equipos, Sistemas de Información e Infraestructura que soportan esta información.
§ Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
· Confidencialidad: Aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello.
· Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento.
· Integridad: Salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas por entes debidamente autorizados.

6. ROLES Y RESPONSABILIDADES

i. Subsecretario: En su calidad de Jefe de Servicio, es el responsable del Sistema de Gestión de Seguridad de la Información de SUBDERE, provee evidencia de su compromiso con el desarrollo y la implementación de este sistema, así como la mejora continua y su efectividad mediante:
Asignar roles y responsabilidades en seguridad de la información.
Establecer y apoyar el Sistema Integrado de Gestión de la SUBDERE. Deberá participar o nombrar un representante que actuará en su nombre.
Proporcionar los recursos necesarios para una adecuada implementación, mantención y mejora del SGSI.
Nombrar el Encargado de Seguridad de la Información institucional.
Comunicar a las y los funcionarios de la Subsecretaría sobre la importancia de lograr los objetivos de seguridad, de cumplir sus responsabilidades y de buscar el mejoramiento continuo en el área de seguridad de la información.
Aplicar sanciones administrativas, en caso de que corresponda, al detectar violaciones o alteraciones al no

acatar lo indicado en las normas, procedimientos y controles emanados de esta política general.

ii. Consejo del Sistema Integrado de Gestión (SIG): Difundir la Política General de Seguridad de la Información y de la documentación que de ella se desprenda. Lo anterior sin perjuicio de las funciones y responsabilidades dispuestas en la Resolución N°2477/2022 del 08 de marzo de 2022, que aprueba la política del SIG.

iii. Comité de Seguridad de la Información: Es el órgano constituido al interior de la SUBDERE e instaurado mediante la presente política, que está encargado de colaborar en la implementación del Sistema de Gestión de Seguridad de la Información en la búsqueda de su adecuado funcionamiento, eficacia y mejora continua. Las funciones de este comité son las siguientes:

Apoyar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en SUBDERE.

Alinear en las distintas áreas de la organización las prioridades y estrategias de seguridad de la información.

Definir el Alcance del Sistema de Gestión de la Seguridad de la Información (SGSI).

Colaborar en el monitoreo y la evaluación de los riesgos de seguridad de la información que afecten a los activos críticos de información.

Conocer la investigación y monitoreo a incidentes de seguridad que afectan a los activos de la información institucionales.

Aprobar políticas específicas sobre seguridad de la información.

Velar por la correcta implementación de las Política General de Seguridad de la Información y de las políticas específicas emanadas de esta, y la revisión permanente de todas ellas.

Generar propuestas para mejorar la seguridad de la información en la SUBDERE.

Proveer de información al Consejo del Sistema Integrado de Gestión (SIG).

Promover la difusión de las Política de Seguridad de la Información y de la documentación relacionada al Sistema de Gestión de la Seguridad de la Información (SGSI).

Este comité estará conformado por las personas encargadas de: Seguridad de la Información, Ciberseguridad, Riesgos; además de un representante del: Comité Informático de SUBDERE (CIS), Departamento de Informática (ámbito de tecnologías de información), Departamento de Administración (ámbito de seguridad física y del entorno) y del Departamento de Gestión y Desarrollo de Personas (ámbito de seguridad de personas).

iv. Encargado de Seguridad de la Información: Funcionaria o funcionario responsable de supervisar todos los aspectos relativos a los temas tratados en la presente Política. Lo anterior sin perjuicio de las funciones y responsabilidades dispuestas en la resolución de nombramiento vigente.

v. Encargado de Ciberseguridad: Funcionaria o funcionario responsable de implementar medidas de ciberseguridad que promueve el Estado y coordinar con el Encargado de Seguridad de la Información las respuestas a incidentes relacionados con la ciberseguridad.

vi. Departamento de Informática: Área encargada de cubrir los requerimientos de seguridad establecidos para la operación, administración, y comunicación de los sistemas y recursos tecnológicos de la SUBDERE.

vii. Departamento de Gestión y Desarrollo de Personas: Área encargada del proceso de inducción a las personas que ingresan a SUBDERE. En ese proceso se debe informar sobre la obligatoriedad de cumplir con la Política General de Seguridad de la Información, y las políticas, normas, procedimientos y controles emanados de esta política general. Además, es el área encargada de gestionar las capacitaciones en materia de seguridad de la información que sean requeridas por las unidades respectivas.

viii. Departamento de Fiscalía: Área encargada de asesorar, en caso de que se requiera, al Comité de Seguridad de la Información en materias de carácter legal relativas a la seguridad de la información.

ix. Dueño de Activo(s) de Información: Es la o el funcionario que debe velar dentro de su respectivo proceso porque el o los activos de información a su cargo cumplan con las políticas, procedimientos, controles, entre otros, que para este efecto SUBDERE establezca.

x. Usuarios y usuarias: Son las personas, funcionarios y funcionarias, practicantes o personal externo que preste servicios permanentes o temporales, que usan los activos de información de la SUBDERE. Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política General de Seguridad de la Información vigente, así como las políticas, procedimientos y controles asociados al SGSI y, además tienen la obligación de reportar cualquier incidente o evento de seguridad del que tengan conocimiento.

xi. Jefaturas de SUBDERE: Las jefaturas de las divisiones, unidades regionales, departamentos y unidades, deberán supervisar que las personas que se encuentran bajo su dependencia cumplan con la presente política, así como las demás políticas, procedimientos, controles, entre otros, emanados de esta política general.

7. DIRECTRICES PARA LA APLICACIÓN DE LA POLÍTICA

7.1 Información Institucional: La información es un activo vital y todos sus accesos, usos y procesamiento, deberán ser consistentes con las políticas y estándares establecidos por SUBDERE en cada ámbito de la seguridad de la información. La información debe ser protegida, por los dueños de los activos de información, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas de seguridad de la información, sus procedimientos asociados y recomendaciones establecidas por SUBDERE.

7.2 Gestión del Riesgo: Cada activo deberá clasificarse según la importancia y la sensibilidad de la información, bajo el modelo de Análisis de Riesgo. Los criterios de estimación del riesgo para el Sistema de Gestión de la Seguridad de la Información (SGSI) corresponden a los establecidos por el Consejo de Auditoría Interna General de Gobierno (CAIGG), mediante la metodología COSO II – ERM, y lo estipulado en la “Guía Metodológica del Programa de Mejoramiento de la Gestión – Sistema de Seguridad de la Información” - Vigente, ambos documentos de aplicación a los Servicios de la Administración Pública Chilena.

7.3 Acciones de mitigación: La Política General de Seguridad de la Información deberá ser complementada con políticas, procedimientos, controles, entre otros, sobre aspectos específicos de la seguridad de la información en el ámbito organizacional, tecnológico, personas, y físico y ambiental, que permita mitigar los riesgos levantados.

La Dirección del Servicio deberá proveer los recursos que permitan implementar los controles necesarios para otorgar el nivel de protección acorde al valor de los activos.

En ese sentido, las acciones deberán apuntar a lo que se desagrega a continuación:

a) Velar porque las y los funcionarios de planta y contrata y el personal a honorarios de la Institución, cuenten con las competencias y conocimiento en materias concernientes a la presente Política y a otra normativa asociada al Sistema de Seguridad de la Información.

b) Asegurar que toda la información y los medios que la contienen, procesen, almacenen, emitan y/o transporten, cumplan con las regulaciones legales vigentes.

c) Fomentar que el procesamiento y almacenamiento de la información se realice mediante una óptima utilización de los recursos disponibles en la Institución.

d) Promover condiciones de ambiente seguro en los lugares de procesamiento y almacenamiento de los activos de información.
e) Garantizar que todos los medios de procesamiento y/o almacenamiento de información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personas no autorizadas.
f) Registrar todas las operaciones realizadas mediante sistemas de información, controlando el acceso físico/lógico a los activos de información.
g) Comprobar y validar periódicamente el funcionamiento seguro de los sistemas de información.
h) Garantizar que la información y la capacidad de procesamiento manual o automático, sean resguardados y recuperados de manera que se mantenga la continuidad operacional.
i) Asegurar que todos los derechos de propiedad sobre los activos de información que sean utilizados estén legalmente establecidos en favor de la Institución.
j) Subsanar los potenciales incidentes de seguridad de los activos de información reportadas por las instancias correspondientes.
k) Implementar medidas asociadas a ciberseguridad de las redes plataformas y sistemas informáticos que son de responsabilidad de la SUBDERE.

8. VINCULACIÓN CON EL SISTEMA INTEGRADO DE GESTIÓN

La presente Política se aplicará de manera complementaria con las demás políticas internas y gubernamentales (CSIRT) definidas para la Subsecretaría, así como otros documentos pertinentes de SUBDERE y debe ser consistente con la Política del Sistema Integrado de Gestión (SIG).

Toda la documentación que forme parte del Sistema de Gestión de Seguridad de la Información (SGSI) se desarrollará bajo los criterios, formatos y metodologías existentes en el marco del SIG.

9. EVALUACIÓN DEL CUMPLIMIENTO

Con el fin de velar por el correcto uso de los recursos, el cumplimiento de esta política, los documentos emanados de ésta y el Sistema de Gestión de Seguridad de la Información (SGSI) en general, serán evaluados periódicamente mediante inspecciones y/o auditorías que correspondan.

10. REVISIÓN DE LA POLÍTICA

La presente Política y todas aquellas que de aquí se desprendan deberán ser revisadas y de ser necesario actualizadas al menos una vez cada 2 años, o cuando ocurran cambios que pudieran afectar el enfoque de la Subsecretaría para la gestión de la seguridad de la información.

11. VULNERACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Cualquier incumplimiento o vulneración de la Política General de Seguridad de la Información, políticas específicas o estándares, se atiene a las sanciones establecidas para los funcionarios del Sector Público, dispuestas en la Ley 18.834 “Estatuto Administrativo” y cuyo texto se refunde en el Decreto con Fuerza de Ley N°29, de fecha de promulgación 16 de junio de 2004 (fecha de publicación 16 de marzo de 2005).

12. EXCEPCIONES

La presente Política y las políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando existan casos con razones fundadas, los cuales serán documentados por el Encargado de Seguridad de la Información y debidamente autorizados por el Jefe de Servicio.

Artículo 2° ACTUALIZACIÓN DEL DOCUMENTO
Se deja constancia que las actualizaciones que considera la presente resolución respecto de la política general de seguridad de la información definida por la Resolución Exenta N°8328/2018 de 2018, de esta Subsecretaría, que por este acto se deja sin efecto, dicen relación con lo siguiente:

· Se modifica la estructura del documento en relación con sus apartados, modificando el orden de estos y cambiando parte o la totalidad de su contenido, además de su redacción.
· Número 1. Objetivo se reemplaza por apartado 1. DECLARACIÓN INSTITUCIONAL.
· En el apartado Documentos de Referencia, se eliminan algunos documentos y se agregan Ley 21.180, normativa sobre ciberseguridad y Resolución Nº2477 que aprueba Política SIG de SUBDERE.
· En el apartado Definiciones, se quitan algunas definiciones y se agregan conceptos de Sistema Integrado de Gestión, Seguridad Informática y Ciberseguridad.
· Se modifica el apartado de Roles y Responsabilidades, agregando el Consejo SIG, Comité de Seguridad de la Información, Encargado de Ciberseguridad, Jefaturas SUBDERE, Usuarios (as). Se elimina a la Unidad de Auditoría Interna, al Comité de Calidad, Riesgos y Seguridad de la Información y se modifican ciertas funciones de algunos roles.
· El apartado Contexto General se elimina y en parte se funde con el apartado 1. DECLARACIÓN INSTITUCIONAL.
· En el apartado Alcance de la presente Política, se elimina gran parte del contenido. En la presente versión se elimina la palabra “presente” del título.
· El apartado Objetivos del Sistema de Gestión de Seguridad de la Información se elimina.
· En el apartado de Criterios generales de aplicación de la Política del SGSI, se elimina 6.3 y 6.4, lo puntos restantes se reordenan y modifican parcialmente (7.1 Información Institucional y 7.2 Gestión del Riesgo). El apartado se pasa a llamar 7. DIRECTRICES PARA LA APLICACIÓN DE LA POLÍTICA, agregando además el apartado 7.3 Acciones de mitigación.
· El apartado 6.5 Violación de las políticas de seguridad de la información pasa a ser el número 11 en la presente versión y pasa a llamarse VULNERACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.
· El apartado 6.6 Auditorías al SGSI pasa a denominarse 9. EVALUACIÓN DEL CUMPLIMIENTO, modificándose parcialmente el contenido de la versión anterior.
· El apartado 6.7 Revisión del presente documento pasa a denominarse 10. REVISIÓN DE LA POLÍTICA.
· Se agrega apartado 2. OBJETIVOS DE LA POLÍTICA, incluyendo números 2.1 OBJETIVO General de la Política y 2.2 sobre Objetivos Específicos.
· Se agrega apartado 8. VINCULACIÓN CON EL SISTEMA INTEGRADO DE GESTIÓN.
· Se agrega apartado 12. EXCEPCIONES.

Artículo 3° DIFUSIÓN DE LA POLÍTICA.

La Difusión de la Política de Seguridad de la Información será responsabilidad del Encargado de Seguridad de la Información de SUBDERE, quien realizará todas las gestiones y acciones que requiera esta política, la que debe ser conocida y asumida por todos los funcionarios de la SUBDERE a quienes se les aplica.
Para ello, se utilizará para este medio correos masivos institucionales (Solosubdere) y la publicación de la presente resolución en la Intranet Institucional.

Artículo 4°.- Dejase sin efecto la Resolución Exenta N° 8328, del año 2018, de esta Subsecretaría sobre la misma materia, a contar de la fecha de total tramitación de la presente resolución.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE EN LA INTRANET INSTITUCIONAL

NICOLAS EDUARDO CATALDO ASTORGA
Subsecretario
Gabinete

NCA/ / EOP/ BND/ FDFT/ LCM/ JHR/ JOM/ IAO/ JHN/ jcl

DISTRIBUCION:
FELIPE MENESES - Asesor - Departamento de Planificación y Gestión
Jefe Departamento (S) - Departamento de Planificación y Gestión
NIEVES DURAN - Jefa Unidad - Oficina de Partes

Firmado Electrónicamente en Conformidad con el Artículo 2º letra F y G de la Ley 19.799