Ministerio de Vivienda y Urbanismo

Gobierno de Chile

MODIFIQUESE LA RESOLUCIÓN EXENTA N°1508, (V. y U.), DE 2023, QUE APRUEBA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO, SUS SERVICIOS DE VIVIENDA Y URBANIZACIÓN, EL PARQUE METROPOLITANO DE SANTIAGO Y LA SUBSECRETARÍA DE VIVIENDA Y URBANISMO (NIVEL CENTRAL Y SUS SECRETARIAS REGIONALES MINISTERIALES).

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA
04 MAR 2025
RESOLUCIÓN EXENTA
TRAMITADA

SANTIAGO, 04 MAR. 2025 HOY SE RESOLVIÓ LO QUE SIGUE

RESOLUCIÓN EXENTA N° Nº . 325

VISTOS: Lo dispuesto en la Ley N° 16.391, que crea el Ministerio de la Vivienda y Urbanismo; el D.L. N°1305 de 1975 que reestructura y regionaliza el Ministerio de Vivienda y Urbanismo; en el D.S. N°83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado sobre la Seguridad y Confidencialidad de los documentos electrónicos; D.S. N°181, de 2012, del Ministerio de Economía, Fomento y Turismo, que aprueba reglamento de la Ley N°19.799 sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha firma; el D.S. N°164 de 2023 que aprobó la Política Nacional de Ciberseguridad 2023-2028; el Instructivo Presidencial N°8 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; el D.S. N°273 de 2022, del Ministerio del Interior y Seguridad Pública, que establece la obligación de reportar incidentes de ciberseguridad; el D.S. N°7, de 2023, del Ministerio Secretaría General de la Presidencia, que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la ley N°21.180; la Resolución Exenta N°1.508 (V. y U.), de 2023, que aprueba la Política General de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo; la Resolución N°1.238, (V. y U.), de 2023 que actualiza la estructura funcional para el Sistema de Seguridad de la Información y Ciberseguridad; la Ley N°21.663, Ley Marco de Ciberseguridad; y la Resolución N°7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón; y,

CONSIDERANDO:

a) Que, el surgimiento de nueva normativa legal, como la Ley N°21.663, que establece un marco en materia de Ciberseguridad e Infraestructura Crítica de la Información; la actualización de los marcos referentes (como la nueva versión de la ISO 27001:2022, NIST CSF 2.0), y la confección de estándares sectoriales relevantes (como la RAN 20-10) generan un desafío constante en los distintos organismos y servicios públicos y sus equipos de seguridad de la información actualizar sus herramientas y metodologías para evaluar o incorporar las nuevas exigencias en sus normativas y regulaciones internas.

b) Que, sumado a lo indicado en el considerando anterior, el marco normativo de la Seguridad de la Información y Ciberseguridad, también considera una serie de normas como el Decreto Supremo N°83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; D.S N°181, de 2002, de Ministerio de Economía, Fomento y Turismo, que aprueba reglamento de la Ley N°19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; el Instructivo Presidencial N°8 de 2018 que imparte instrucciones en materias de Ciberseguridad a los órganos de la administración del Estado la Política Nacional de Ciberseguridad de 2023; el D.S. N°164 de 2023 que aprobó la Política Nacional de Ciberseguridad 2023-2028; el D.S. N°7, de 2023, del Ministerio del Interior y Seguridad Pública, que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme lo establecido en la Ley N°21.180, entre otras.

c) Que, en conformidad a lo dispuesto en el numeral 6.4 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo, aprobada por medio de la Resolución Exenta N°1508, (V. y U.), de 2023, indica que: *"La presente política será revisada al menos una vez al año o cuando el/la Encargado/a de Seguridad de la Información y Ciberseguridad de uno o más Servicios lo requiera, para asegurar su continuidad e idoneidad, considerando los resultados de revisiones y auditorías realizadas, y los cambios que puedan producirse, tales como:*

- *Nuevas definiciones estratégicas, cambios en la institución y/o enfoques a la gestión de seguridad.*
- *Incorporación y/o modificaciones relevantes de procesos o actividades críticas de la institución.*
- *Cambios significativos al soporte tecnológico.*
- *Cambios significativos en los niveles de riesgo a que se expone la información.*
- *Modificación y/o creación de leyes o reglamentos que afecten la institución.*
- *Recomendaciones realizadas por autoridades pertinentes.*

- *Tendencias relacionadas con amenazas y vulnerabilidades".*

d) Que, en mérito de lo anterior dicto la siguiente:

RESOLUCIÓN:

1.- MODIFÍQUESE la Resolución Exenta N°1508, (V. y U.), de 08 de septiembre de 2023, referida en los considerandos de esta resolución, en el sentido de reemplazar todos sus considerandos por los siguientes:

a) *Que, el surgimiento de nueva normativa legal, como la Ley N°21.663, que establece un marco en materia de Ciberseguridad e Infraestructura Crítica de la Información, pero que aún no se encuentra vigente; la actualización de los marcos referentes (como la nueva versión de la ISO 27001:2022, NIST CSF 2.0), y la confección de estándares sectoriales relevantes (como la RAN 20-10) generan un desafío constante en los distintos organismos y servicios públicos y sus equipos de seguridad de actualizar sus herramientas y metodologías para evaluar o incorporar las nuevas exigencias en sus normativas y regulaciones internas.*

b) *Que, sumado a lo indicado en el considerando anterior, el marco normativo de la Seguridad de la Información y Ciberseguridad, también considera una serie de normas como el Decreto Supremo N°83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; D.S N°181, de 2002, de Ministerio de Economía, Fomento y Turismo, que aprueba reglamento de la Ley N°19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; el Instructivo Presidencial N°8 de 2018 que imparte instrucciones en materias de Ciberseguridad a los Órganos de la Administración del Estado la Política Nacional de Ciberseguridad de 2023; el D.S. N°164 de 2023 que aprobó la Política Nacional de Ciberseguridad 2023-2028; el D.S. N°7, de 2023, del Ministerio del Interior y Seguridad Pública, que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme lo establecido en la Ley N°21.180, entre otras.*

c) *Que, en conformidad a lo dispuesto en el numeral 6.4 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo, aprobada por medio de la Resolución Exenta N°1508, (V. y U.), de 2023, indica que: "La presente política será revisada al menos una vez al año o cuando el/la Encargado/a de Seguridad de la Información y Ciberseguridad de uno o más Servicios lo requiera, para asegurar su continuidad e idoneidad, considerando los resultados de revisiones y auditorías realizadas, y los cambios que puedan producirse, tales como:*

- *Nuevas definiciones estratégicas, cambios en la institución y/o enfoques a la gestión de seguridad.*

- *Incorporación y/o modificaciones relevantes de procesos o actividades críticas de la institución.*
- *Cambios significativos al soporte tecnológico.*
- *Cambios significativos en los niveles de riesgo a que se expone la información.*
- *Modificación y/o creación de leyes o reglamentos que afecten la institución.*
- *Recomendaciones realizadas por autoridades pertinentes.*
- *Tendencias relacionadas con amenazas y vulnerabilidades.*

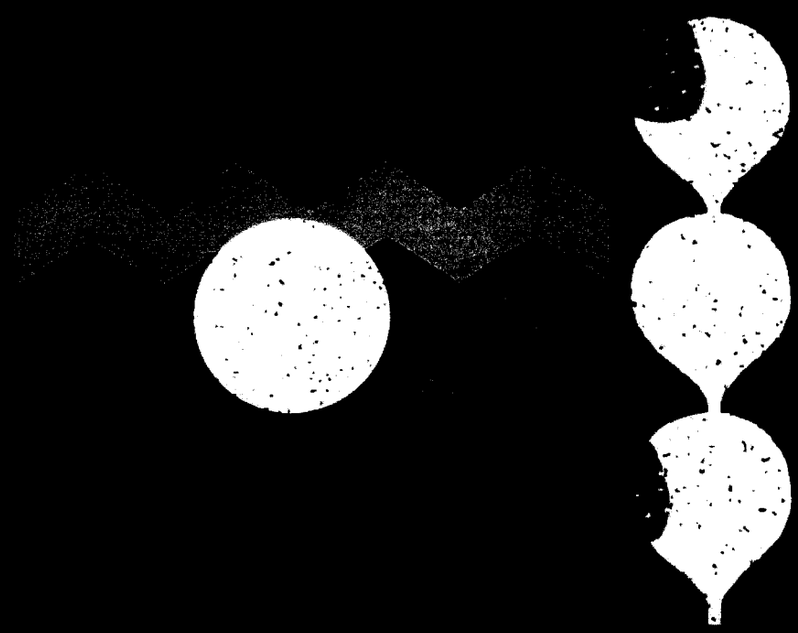
d) *Que, en mérito de lo anterior dicto la siguiente:*

2.- MODIFÍQUESE la Resolución Exenta N°1508, (V. y U.), de 08 de septiembre de 2023, en su parte resolutiva, en el sentido de reemplazar su resuelvo II por el siguiente:

II.- APRUEBESE *la Política General de Seguridad de la Información y Ciberseguridad del Ministerio de Vivienda y Urbanismo, que rige a la Subsecretaría de Vivienda y Urbanismo, las Secretarías Regionales Ministeriales de Vivienda y Urbanismo; los Servicios de Vivienda y Urbanización y el Parque Metropolitano de Santiago, que se detalla a continuación:*

Política de Seguridad de la Información y Ciberseguridad

Ministerio de Vivienda y Urbanismo



Ministerio de Vivienda y Urbanismo

Gobierno de Chile

CONTENIDO

Nota: En el contenido del documento se identifican los cambios respecto a la versión anterior en negrita y cursiva

0. GLOSARIO

Activo	***Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio, sea a otras instituciones de la Administración del Estado o con personas naturales o jurídicas.***
Activo de Información	***Datos o información cuyo tratamiento es esencial para el desarrollo de las funciones propias de la institución que lo utiliza, genera, almacena, envía o intercambia, y que deben ser protegidos en su confidencialidad, integridad, disponibilidad u otros factores de importancia. Los activos de información pueden tener formato físico, electrónico o verbal, ser equipos o aplicativos, o incluso las personas cuyo conocimiento sirve para lograr los propósitos u objetivos de la Institución.***
Ciberseguridad y Seguridad de la Información	***Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de los órganos de la Administración del Estado, aumentando su resiliencia en el tiempo.***
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Control de Seguridad	***Conjunto de estándares, buenas prácticas y normativas que permiten administrar los riesgos en las tecnologías de la información.***
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad o proceso autorizada.
Documento de Aplicabilidad	***Declaración documentada que describe los controles que son relevantes para el Sistema de Gestión de la Seguridad de la Información, en adelante, SGSI, de la organización y aplicables al mismo, así como el rol de cada institución del Ministerio de Vivienda y Urbanismo.***
Gestión de Riesgo	***Proceso estructurado y proactivo por el cual se identifican, evalúan, controlan y tratan los riesgos derivados de una o más amenazas determinadas.***
Incidente de Seguridad de la Información	***Todo evento de seguridad o una serie de ellos, de carácter no deseado o inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos***

	y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan comprometer las operaciones del negocio, la continuidad del servicio y amenazar la seguridad de la información.
Información	Toda comunicación o representación de conocimiento como datos, en cualquier forma, tales como formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea digital, en papel, audiovisual u otro.
Integridad	***Propiedad de mantener la información con exactitud, autenticidad y completitud.***
Plataforma electrónica (en adelante también "plataforma")	***Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.***
Riesgo	***Efecto de la incertidumbre sobre los activos de información y los objetivos de una entidad, habitualmente expresado en relación con las consecuencias de un evento o incidente de seguridad y su probabilidad de ocurrencia.***
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Servidor	***Equipo virtual o físico dedicado a entregar servicios de red, servicios de bases de datos, sitios web, sistemas informáticos, carpetas compartidas y, en general, brindar los recursos necesarios para responder las peticiones de usuarios.***
Sistema de Gestión de Seguridad de la Información (SGSI)	La parte del sistema de gestión general, basada en un enfoque de riesgo organizacional, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Este incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.
Usuarios(as)	***Funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo empresas que presten servicios en el Ministerio de Vivienda y Urbanismo, en la Subsecretaría de Vivienda y Urbanismo, en las Secretarias Regionales Ministeriales, en los Servicios de Vivienda y Urbanismo y el Parque Metropolitano de Santiago.***

1. DECLARACIÓN INSTITUCIONAL

El Ministerio de Vivienda y Urbanismo -MINVU- se ha comprometido a establecer, mantener y mejorar continuamente un Sistema de Seguridad de la Información ***y Ciberseguridad***-en adelante el SSI-, ***y un modelo de Gobernanza de Datos***, siendo éste un *"compromiso en el fomento y desarrollo de una cultura de la seguridad, basado en preservar los principios de confidencialidad, integridad y disponibilidad de la información, en beneficio de la ciudadanía y partes interesadas para alcanzar los objetivos institucionales, contribuyendo al fortalecimiento del Derecho a la Ciudad y a una Vivienda Digna y Adecuada, con enfoque territorial y perspectiva de género, poniendo énfasis en la ejecución del Plan de Emergencia Habitacional, el Mejoramiento de Viviendas y Entornos para vivir en Comunidad, la Construcción de Ciudades Justas para el encuentro ciudadano, la recuperación de suelo e inmuebles para las familias y la Modernización de la gestión".*

Por tal motivo la información es un activo esencial para que el MINVU avance hacia el cumplimiento de su misión ministerial, entendiendo por Activo de Información, todos aquellos elementos que hacen posible o sustentan los procesos operacionales, como las personas que utilizan la información; los equipos, sistemas e infraestructura que soporta la información; ***los datos que se generan;*** y la información propiamente tal en cualquiera de sus múltiples formatos.

Para el desarrollo del SSI, la presente política general, las políticas específicas, procedimientos y otros documentos relacionados, se ajustan a los requerimientos normativos vigentes en Seguridad de la Información, además de considerar los aspectos pertinentes del marco normativo del MINVU[1].

2. OBJETIVO GENERAL

El objetivo de este documento es:

- Establecer los lineamientos institucionales y entregar orientación en ***materias de*** Seguridad de la Información ***y Ciberseguridad y Gobernanza de Datos dentro*** del Ministerio de Vivienda y Urbanismo.
- Definir los objetivos y principios para guiar las actividades relacionadas con la seguridad de la información ***y la gobernanza de datos***, con el fin de contar con información precisa, completa, y disponible de manera oportuna y así permitir el logro de los objetivos institucionales, la eficiencia de los procesos y el cumplimiento de la legislación.

2.1 Objetivos específicos de la Seguridad de la Información, *Ciberseguridad y Gobernanza de Datos*

El Sistema de Seguridad de la Información del MINVU **y el Modelo de Gobernanza de Datos** se alinean y permiten soportar los objetivos estratégicos ministeriales definidos en la Ficha de Definiciones Estratégicas A0[2]. La institución establece los siguientes objetivos de la gestión de seguridad de la información:

- Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la Seguridad de la Información.

---

[1] Disponible en www.minvu.cl, enlace "Marco Normativo".

[2] Los objetivos estratégicos ministeriales se encuentran disponibles en la Ficha de Definiciones Estratégicas (Formulario A0) publicado en la Intranet del MINVU.

A0[2]. La institución establece los siguientes objetivos de la gestión de seguridad de la información:

- Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la Seguridad de la Información.
- Establecer los niveles de acceso apropiados a la información, brindando y asegurando la ***preservación de la*** confidencialidad, integridad y disponibilidad que requiera cada sistema, proceso, actividad crítica y usuario.
- Apoyar el modelo ***y/o procesos referente*** a las gestiones tendiente a asegurar la continuidad de negocio, a través de acciones tendientes a gestionar los incidentes y a revertir y resolver contingencias que se detecten.
- Establecer un marco de Gestión de Riesgo Cibernético para cada sistema, proceso, actividad crítica, que permita alcanzar los objetivos estratégicos.

Para lo anterior, en el marco del SSI, se establecen un conjunto de controles aplicables, seleccionados a través de un proceso de gestión de riesgos y la formalización de políticas, procesos, procedimientos para proteger los activos de información en consistencia con los principios establecidos en el punto 5 de esta política.

3. ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD Y DEL SSI – ALCANCE

La presente política es aplicable a todos los procesos[3] vinculados a los objetivos ministeriales y productos estratégicos del MINVU.

Asimismo, esta política es aplicable a funcionarios de planta, contrata y honorarios, en adelante también *"el personal"*, que forman parte del Ministerio de Vivienda y Urbanismo, de la Subsecretaría de Vivienda y Urbanismo, las Secretarias Regionales Ministeriales, así como de los servicios que se relacionan con esta Secretaría de Estado, es decir, los Servicios de Vivienda y Urbanización y el Parque Metropolitano de Santiago, incluyendo a asesores, consultores, practicantes y personas naturales o jurídicas, que se relacionen o que se encuentran vinculadas con el MINVU en virtud de contratos, convenios, normativa vigente, entre otros. En el caso de *"el personal"*, les aplica indistintamente de la modalidad de trabajo que realice, ya sea *"presencial"*, *"a distancia"*, *"teletrabajo"* u otra, en las condiciones que establezca la legislación vigente.

Para dar cumplimiento a los requisitos, el MINVU establecerá un conjunto de normas, directrices, procedimientos, instructivos y herramientas de seguridad que permitirán mitigar los riesgos que pudiesen afectar la protección de los activos de información. Esta documentación estará disponible para todo el personal del MINVU en la intranet institucional.

Esta Política genera el marco ministerial de Seguridad de la Información; sin embargo, cada Servicio puede definir las políticas específicas que considere necesarias y que sean de aplicación local; estos documentos no pueden contener elementos que contravengan la presente política, aplicándose además esta última en todos los aspectos no regulados por aquellas.

---

[2] Los objetivos estratégicos ministeriales se encuentran disponibles en la Ficha de Definiciones Estratégicas (Formulario A0) publicado en la Intranet del MINVU.

[3] Los procesos se encuentran definidos en el Mapa de Procesos Ministerial.

4. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades para el SSI son definidos por cada Servicio, en cuanto al contenido específico de su composición y funciones, mediante la formalización de un acto administrativo que considera al menos:

- **Encargado/a de Seguridad de la Información**: cuyo rol asesora a la jefatura de cada Servicio en materias relativas a Seguridad de la Información y Ciberseguridad, coordinar las acciones tendientes a cumplir y apoyar los objetivos de seguridad de la información y lidera la identificación de amenazas o riesgos en la seguridad de la información o de sus instalaciones.
- **Comité de Seguridad de la Información** o Comité de similar denominación: formado por un equipo multidisciplinario de alto nivel en cada Servicio que tiene injerencia en las decisiones estratégicas relativas a la seguridad de la información, así como también en la supervisión y monitoreo del SSI.
- ***Encargado/a de Activos de Información, quien será el (la) responsable de su identificación y clasificación, así como gestionar el riesgo y niveles de seguridad asociados, en conformidad a lo dispuesto en el artículo 5° del Decreto Supremo N°7 de 2023, del Ministerio del Interior y Seguridad Pública.***

Cabe destacar que los usuarios, funcionarios de planta, contrata y honorarios que forman parte del Ministerio de Vivienda y Urbanismo, así como también asesores, consultores, practicantes y personas naturales o jurídicas que prestan servicios para el MINVU, son responsables de cumplir las políticas de seguridad de la información del MINVU, asegurar la confidencialidad, disponibilidad e integridad de la información que tienen a su cargo y reportar oportunamente los incidentes de seguridad de la información que detecten en el desarrollo de sus funciones.

5. PRINCIPIOS PARA EL RESGUARDO DE LOS ACTIVOS DE INFORMACIÓN

La seguridad de la información es el conjunto de medidas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger los Activos de Información, buscando mantener la confidencialidad, la disponibilidad e integridad de éstos.

A continuación, se describe cómo el MINVU aborda los principios básicos de Seguridad de la Información:

5.1 De la confidencialidad de los activos de información

El MINVU se compromete a preservar la confidencialidad de la información institucional, estableciendo lineamientos, prácticas de seguridad y mecanismos para clasificar y reconocer la información de carácter confidencial en la gestión interna, que deba ser protegida ante filtración o divulgación no autorizada. Esta clasificación es de carácter interna y diferente de la tipificación del carácter reservado de la información, la cual se encuentra a cargo del equipo de Transparencia en cada Servicio, quienes resguardan el Principio de Transparencia de la función pública[4] recogido en la Ley N°20.285 sobre Acceso a la Información Pública.

Por lo anterior, y dada la condición pública de la información elaborada con presupuesto de la nación y que obra en poder de los Órganos de la Administración del Estado, es importante señalar que su

[4] Artículo 5 de la Ley 20.285, que establece el carácter público de la información de los órganos de la Administración del Estado.

resguardo no implica desconocimiento ni obstaculización del derecho de toda persona a solicitar y recibir información, en la forma y condiciones que establece la Ley N°20.285.

Además, el resguardo de la información involucra la obligación de las personas que trabajan en el tratamiento de datos personales o que tengan acceso a estos, de guardar secreto sobre los mismos, según lo dispone la Ley N°19.628 de Protección de Datos de Carácter Personal.

De este modo, cada Servicio se compromete a implementar los controles necesarios para garantizar que, tanto la información física como la digital, sea accesible sólo por aquellos usuarios autorizados de acuerdo con la legislación vigente, revisando periódicamente estos lineamientos ***y considerando el ciclo de vida de los activos de información.***

5.2 De la integridad de los activos de información

El MINVU establece lineamientos, prácticas de seguridad y mecanismos que resguardan la integridad de los Activos de Información contenida en cualquier espacio, equipo, sistema o infraestructura, en todos los formatos posibles, salvaguardando además la mayor completitud, coherencia, consistencia y actualización de sistemas y procesos.

5.3 De la disponibilidad de los activos de información

El MINVU asegura la disponibilidad de los Activos de Información ministerial, incluyendo la disponibilidad de equipos, sistemas e infraestructura que la contengan o la provean en los niveles y tiempos requeridos, tanto a escala interna como externa, estableciendo lineamientos, prácticas de seguridad y mecanismos que prevengan cualquier acción que ***interrumpa*** la continuidad del flujo de información.

6. GESTIÓN DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN *Y CIBERSEGURIDAD*

6.1 Generación de una política y otros documentos

La Política de Seguridad de la Información ***y Ciberseguridad*** se elaboran en base a un formato tipo establecido para dicho propósito publicado en la columna Trabajo Colaborativo SSI en la Intranet institucional. Asimismo, para la implementación operativa de algunas políticas específicas de seguridad, se elaboran procedimientos u otros instrumentos que se alinean con los parámetros establecidos de documentación en cada Servicio.

6.2 Aprobación de una política y otros documentos

La Política General y las Políticas Específicas de Seguridad son aprobadas a través de un acto administrativo suscrito por el Jefe de Servicio, facultad que no puede ser delegada.

Los demás documentos que se requiera emitir, como normativas, procedimientos e instructivos son aprobados a través de un acto administrativo igualmente suscrito por el Jefe de Servicio, o por aquellos funcionarios en quienes haya sido delegada dicha atribución, dependiendo de los lineamientos y prácticas de seguridad particulares o transversales definidos en cada Servicio, conforme a su estructura y

con lo establecido por cada Servicio, asegurando que el contenido de la documentación sea accesible y comprensible para todo el personal del MINVU.

La difusión de la presente política, las políticas específicas de seguridad, los procedimientos y otros documentos, se deberá efectuar a través de los canales de difusión establecidos, pudiendo utilizarse publicación en el ***sitio "Sistema de Seguridad de la Información"*** y/o Minvuletín y/o Correo electrónico y/o Afiches y/o volantes, u otro medio que la institución considere pertinente ***para lograr la difusión del presente instrumento.***

Adicionalmente, tanto la política general como las políticas específicas de seguridad de la información ***de aplicación transversal a todos los Servicios dependientes del MINVU*** se encuentran publicadas en la página web institucional disponible para consulta de personal o terceras partes que prestan servicios para el MINVU y para la ciudadanía en general.

6.4 Revisión de la Política *de Seguridad de la Información y Ciberseguridad*

La presente política será revisada al menos una vez al año o cuando el/la ***Encargado/a de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos (o similar)*** de uno o más Servicios lo requiera, para asegurar su continuidad e idoneidad, considerando los resultados de revisiones y auditorías realizadas, y los cambios que puedan producirse, tales como:

- Nuevas definiciones estratégicas, cambios en la institución y/o enfoques a la gestión de seguridad.
- Incorporación y/o modificaciones relevantes de procesos o actividades críticas de la institución.
- Cambios significativos al soporte tecnológico.
- Cambios significativos en los niveles de riesgo a que se expone la información.
- Modificación y/o creación de leyes o reglamentos que afecten a la institución.
- Recomendaciones realizadas por autoridades pertinentes.
- Tendencias relacionadas con amenazas y vulnerabilidades.

Asimismo, cada Servicio evaluará el cumplimiento de la presente política general, a lo menos cada tres años, mediante auditorías internas, externas y/o revisiones independientes.

7. SANCIONES APLICABLES

El incumplimiento ***o infracción*** de esta Política de Seguridad de la Información ***y Ciberseguridad, por parte de los funcionarios del MINVU, SEREMI, SERVIU y PARQUEMET, acarrea responsabilidad administrativa, debiendo aplicarse alguna de las medidas disciplinarias previstas en el Estatuto Administrativo (censura, multa, suspensión o destitución),*** previa ***instrucción*** y sustanciación del respectivo ***Procedimiento Administrativo Disciplinario***; o el término anticipado del contrato por incumplimiento de las obligaciones que el mismo contempla, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política. Lo anterior, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

8. CONTROL DE VERSIONES

Versión	Fecha Aprobación	Motivo de la revisión	Autor(es)
09	Julio 2023	Revisión anual. Se identifican los cambios en negrita y cursiva.	Ivonne Valdivia / DIVAD; Marcela Jara/ DIFIN; Tomás Yanquez/DIFIN; Leonardo Cavieres/ DINFO; Claudio Paredes/ DINFO; Erick Atenas/ DINFO; M. Paula Melis Otonel/ Contralora Interna SERVIU Araucanía; Alexis Cornejo Marín/ Unidad de Informática SERVIU Atacama; Marcelo López Otárola/ Depto. Programación Física y Control SERVIU BioBío.
10	Enero 2025	Revisión anual. Se incorporan aspectos del D.S. N°7, de 2023, del Ministerio Secretaría General de la Presidencia, que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N°21.180, y cambios de redacción.	Ivonne Valdivia / DIVAD; Litsi Contreras / DIJUR; Marcela Jara / DIFIN; Leonardo Cavieres / DINFO; Claudio Paredes / DINFO; Erick Atenas / DINFO; Gladys Martin / CIM; M. Paula Melis Otonel / Contralora Interna SERVIU Araucanía.
Revisión:			Carlos Araya Salazar/ Subsecretario de Vivienda y Urbanismo (S). Vania Navarro Morales/ ***Encargada de Seguridad de la Información y Ciberseguridad y Gobernanza de Datos, Jefa División de Finanzas*** ***Comité de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos Subsecretaría de V. y U.*** Encargados/as de Seguridad de la Información de SERVIU y Parque Metropolitano de Santiago.
Aprobación:			Carlos Montes Cisternas / Ministro de Vivienda y Urbanismo.

3.- MODIFÍQUESE la Resolución Exenta N°1508, (V. y U.), de 08 de septiembre de 2023, referida en los considerandos de esta resolución, en el sentido de reemplazar su resuelvo III y IV por el siguiente:

II.- INSTRUYASE *a las/os Encargadas/os de Seguridad de la Información y Ciberseguridad de la Subsecretaría de Vivienda y Urbanismo, de las Secretarías Regionales Ministeriales de Vivienda y Urbanismo, de los Servicios de Vivienda y Urbanización y del Parque Metropolitano de Santiago, de llevar acabo la difusión y sociabilización de la política fijada en este instrumento a todos los equipos de trabajo y funcionarios, así como de ejecutar todas las acciones tendientes a su implementación y velar por su estricto cumplimiento.*

III.- DEJESE *constancia que la presente Resolución no irroga gastos para el presupuesto de este Ministerio, ni para los Servicios que se relacionan con el Gobierno por su intermedio.*

4.- MANTENGASE en todo lo no modificado por esta resolución, la Resolución Exenta N°1508, (V. y U.), de 08 de septiembre de 2023.

ANÓTESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.

CARLOS MONTES CISTERNAS
MINISTRO DE VIVIENDA Y URBANISMO

CAS/CGB/MAM/RDC/PMG/VNM/MJC/

DISTRIBUCION:
- Gabinete Ministro V. y U.
- Gabinete Subsecretaria V. y U.
- SEREMI (16)
- Directores/as SERVIU (16)
- Director/a PARQUEMET
- Divisiones Nivel Central (7)
- Auditoría Interna Ministerial
- Contraloría Interna Ministerial
- Comisión Asesora para la Reducción de Riesgos de Desastres y Reconstrucción
- Sistema Integrado de Atención a la Ciudadanía (SIAC)
- Depto. Comunicaciones
- Centro de Estudios de Ciudad y Territorio (CECYT)
- Equipo de Estudios Económicos y de Procesos-DIFIN
- Sección Partes y Archivos

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

GABRIELA ELGUETA POBLETE
SUBSECRETARIA DE VIVIENDA Y URBANISMO