Ministerio de Vivienda y Urbanismo

Gobierno de Chile

une la Ciudad

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE VIVIENDA Y URBANISMO

VERSIÓN 08

MINISTERIO DE VIVIENDA Y URBANISMO
DIRECTOR REGIONAL
SERVIU X^a REGION

Contenido

0. GLOSARIO

Activo de Información	Todo elemento, sea tangible o no, que contenga datos que sean relevantes para el Ministerio, que se encuentren en formato físico o electrónico, sean equipos o aplicativos, o incluso las personas cuyo conocimiento sirve para los propósitos de la Institución.
Confidencialidad[1]	Propiedad de la información por la que no está disponible o divulgada a personas, entidades o procesos no autorizados.
Continuidad del Negocio	Persistencia de las operaciones de la institución.
Disponibilidad[1]	Propiedad de la información, que se traduce en que las personas o procesos autorizados puedan acceder a ella cuando lo requieran.
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 -en lo sucesivo, MINVU-, en la implementación de los controles de la norma ISO 27001:2013.
Incidente de Seguridad de la Información	Evento no deseado o inesperado que tiene una probabilidad significativa de comprometer las operaciones de la institución 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[1]	Propiedad de mantener la información con exactitud y completitud.
Seguridad de la Información[1]	Preservación de la confidencialidad, integridad y disponibilidad de la información.
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.

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

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA
ABOGADA
DIVISIÓN JURÍDICA

[1] Fuente: ISO/IEC 27000:2018

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. DECLARACIÓN INSTITUCIONAL

El Ministerio de Vivienda y Urbanismo -MINVU- ha decidido establecer, implementar, mantener y mejorar continuamente un Sistema de Seguridad de la Información -en adelante el SSI-, siendo éste un *"compromiso en el fomento y desarrollo de una cultura de seguridad, basado en preservar los principios de confidencialidad, integridad y disponibilidad de la información y asegurar la continuidad operacional, en beneficio de los usuarios, ciudadanos y partes interesadas para alcanzar los objetivos institucionales, contribuyendo al desarrollo del país en los ámbitos de ciudad y territorio, barrio y vivienda".*

De este modo, la información es un activo esencial para que el MINVU alcance sus objetivos con el propósito de cumplir con su misión ministerial. Por tal motivo, entendemos por activo de información todos aquellos elementos que hacen posible o sustentan los procesos operativos o de negocio, como las personas que utilizan la información; los equipos, sistemas e infraestructura que soporta la información; y la información propiamente tal en cualquiera de sus múltiples formatos, incluyendo ***soporte*** papel y digital.

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[2].

2. OBJETIVO

El objetivo de este documento es:

- ***Establecer los lineamientos institucionales y entregar orientación en la implementación del Sistema de Seguridad de la Información del MINVU.***
- ***Definir los objetivos y principios para guiar las actividades relacionadas con la seguridad de la información, resguardando la confidencialidad, integridad y disponibilidad de sus activos relevantes, con el fin de mantener la continuidad operacional en los procesos de provisión de bienes y servicios estratégicos en concordancia con la normativa vigente en materias de Seguridad de la Información y Ciberseguridad de manera de cumplir eficientemente con los objetivos estratégicos del Ministerio de Vivienda y Urbanismo.***

2.1 Objetivos de la Seguridad de la Información

El Sistema de Seguridad de la Información del MINVU se alinea y permite soportar los objetivos estratégicos ministeriales definidos en la Ficha de Definiciones Estratégicas A0 [3], para lo cual cuenta con los siguientes objetivos de la gestión de seguridad de la información:

- Resguardar los activos de información mediante controles de seguridad aplicables a partir del análisis, evaluación y tratamiento de los riesgos que afecten su confidencialidad, integridad y disponibilidad.
- Asegurar la continuidad del negocio a través de acciones tendientes a gestionar los incidentes y a revertir y resolver contingencias que se detecten.

Para lo anterior, en el marco del SSI, se establecen un conjunto de lineamientos y prácticas de seguridad de la información en consistencia con las disposiciones indicadas en esta política en el punto 5, debiendo ser formalizadas a través de políticas específicas, procedimientos y otros documentos para su cumplimiento y aplicación por parte de las personas, especialmente en los procesos definidos en el alcance.

MINISTERIO DE VIVIENDA Y URBANISMO CARMEN GLORIA BARRERA ABOGADA DIVISIÓN JURÍDICA

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

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

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

La presente política es aplicable a los procesos asociados a los productos estratégicos que forman parte del SSI en cada Servicio[4] del MINVU.

Esta definición de procesos es formalizada/actualizada anualmente en cada Servicio por su respectivo Comité de Seguridad de la Información, quedando establecida dicha definición en el Acta de reunión.

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, o se relacionan con esta Secretaría de Estado, esto es, la Subsecretaría de Vivienda y Urbanismo (Nivel Central y sus 16 SEREMI), los 16 SERVIU y el Parque Metropolitano de Santiago, así como también a asesores, consultores, practicantes y personas naturales o jurídicas que prestan servicios para el MINVU.

Para el desarrollo del SSI, se consideran los requisitos de la norma NCh-ISO 27001:2013, así como los requisitos regulatorios y legales aplicables identificados en el documento Catastro Normativa MINVU.

La NCh-ISO 27001:2013 establece dominios y controles que se deben cumplir en el marco de un Sistema de Gestión de la Seguridad de la Información (SGSI). Estos dominios han sido considerados en el SSI del MINVU y corresponden a los siguientes:

1. *Políticas de Seguridad de la Información*
2. *Organización de la Seguridad de la Información*
3. *Seguridad ligada a los Recursos Humanos*
4. *Administración de Activos*
5. *Control de Acceso*
6. *Criptografía*
7. *Seguridad Física y del Ambiente*
8. *Seguridad de las Operaciones*
9. *Seguridad de las Comunicaciones*
10. *Adquisición, desarrollo y mantenimiento del Sistema*
11. *Relaciones con el Proveedor*
12. *Gestión de Incidentes de Seguridad de la Información*
13. *Aspectos de la Seguridad de la Información en la gestión de la continuidad del negocio*
14. *Cumplimiento*

Para estos dominios, se 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 tiene su propio sistema de Seguridad de la Información y puede definir las políticas específicas que considere necesarias y que sean de aplicación local; éstos documentos no pueden contener elementos que contravengan la presente política, aplicándose además esta última en todos los aspectos no regulados por aquellas.

Existen algunos controles que son abordados en forma transversal, que producto de la dependencia Tecnológica de SERVIU y PMS con la Subsecretaría de V. y U. se tratan desde Nivel Central. Para orientar al respecto el MINVU cuenta con un "Documento de Aplicabilidad", publicado en la Intranet, en el cual se identifican los controles de la norma ISO 27001:2013, su aplicabilidad institucional y el rol de la Subsecretaría, los SERVIU y el PMS en su implementación.

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA
ABOGADA
DIVISIÓN JURÍDICA

[4] El término "Servicio" hace referencia a la Subsecretaría de Vivienda y Urbanismo (Nivel central y 16 SEREMI), a 16 SERVIU y al Parque Metropolitano de Santiago (PMS).

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**: en cuyo rol el Jefe de cada Servicio delega las decisiones relativas a la seguridad de la información y su coordinación, asegurando la alineación del SSI y sus objetivos al cumplimiento de los objetivos estratégicos, coordinando las acciones necesarias para satisfacer los requisitos aplicables, favoreciendo la ***mejora continua del sistema*** y la satisfacción de las partes interesadas. ***Este Encargado/a es responsable de la correcta aplicación de esta política y su periódica revisión.***
- **Comité de Seguridad de la Información**, o Comité de similar denominación: formado por un equipo multidisciplinario de cada Servicio que tiene injerencia en las decisiones estratégicas relativas a la seguridad de la información, a partir de los dominios que regulan los diferentes aspectos.

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. DISPOSICIONES PARA RESGUARDAR 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 la misma.
A continuación, se describe cómo el MINVU aborda estos 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[5] 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 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 y de acuerdo a la legislación vigente, revisando periódicamente estos lineamientos.

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

MINISTERIO DE VIVIENDA Y URBANISMO CARMEN GLORIA BARRERA ABOGADA DIVISIÓN JURÍDICA

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

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 elimine o exponga la información relevante y que mantengan la continuidad del flujo de información.

6. DISPOSICIONES PARA ASEGURAR LA CONTINUIDAD DEL NEGOCIO

El MINVU busca asegurar que la comunidad vinculada disponga de los servicios e información, de manera oportuna y cuando esta sea requerida según la normativa vigente. Para ello procura que los servicios otorgados a las personas sean resguardados y recuperados en forma adecuada y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento o equipamiento de procesamiento.

7. GESTIÓN DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

7.1 Generación de una política y otros documentos

Las políticas de seguridad de la información 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.

7.2 Aprobación de una política y otros documentos

Las políticas específicas de seguridad son aprobadas a través de resolución del Jefe de Servicio, ***facultad que no puede ser delegada.***

Otros documentos como normativas, procedimientos e instructivos son aprobados a través de un acto administrativo (Resolución) del 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 requerimientos de seguridad.

7.3 Difusión de una política y otros documentos

Las versiones vigentes de la presente política y aquella documentación vinculada al Sistema de Seguridad de Información se publica de acuerdo a 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 efectúa a través de los canales de difusión establecidos, pudiendo utilizarse publicación en la Intranet institucional y/o Minvuletín y/o Correo electrónico y/o Afiches y/o volantes, u otro medio que la institución considere pertinente.

7.4 Revisión de la política

La presente política será revisada anualmente o cuando ***el/la Encargado/a de Seguridad de la Información de uno o más Servicios lo requiera***, para asegurar su continuidad e idoneidad, considerando los cambios que puedan producirse, tales como: enfoques a la gestión de seguridad, circunstancias de la Institución, cambios legales, cambios en el ambiente técnico, recomendaciones realizadas por autoridades pertinentes, tendencias relacionadas con amenazas y vulnerabilidades, entre otras.

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.

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA
ABOGADA
DIVISION JURIDICA

8. SANCIONES APLICABLES

El incumplimiento o violación a esta política, conlleva, en el caso de funcionarios del MINVU, ***la aplicación de alguna de las medidas disciplinarias previstas en el Estatuto Administrativo (censura, multa, suspensión o destitución), previa sustanciación del respectivo proceso disciplinario y en la medida que se acredite en el marco del mismo, responsabilidad administrativa por incumplimiento o violación de esta política; 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.

9. CONTROL DE VERSIONES

Versión	Fecha Aprobación	Motivo de la revisión	Autor(es)
06	Octubre 2017	Revisión anual, considera nuevos requerimientos Red de Expertos. Se identifican los cambios en negrita y cursiva.	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Claudio Paredes/ Jefe de Ingeniería y Explotación de Sistemas DINFO; Ivonne Valdivia / Profesional Depto. Estudios DIVAD; Viviana Peña / Analista Sección Gestión de Procesos DIFIN; Marcela Jara/ Encargada Sección Gestión de Procesos DIFIN.
07	Octubre 2018	Revisión anual, considera ajuste en la aprobación de documentos por observación formulada por Contraloría General de la República. Se identifican los cambios en negrita y cursiva.	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Claudio Paredes/ Jefe de Ingeniería y Explotación de Sistemas DINFO; Ivonne Valdivia / Profesional Depto. Estudios DIVAD; Marcela Jara/ Encargada Sección Gestión de Procesos DIFIN.
08	Julio 2019	Revisión anual, considera ajuste en la aprobación de documentos y algunas especificaciones por recomendación de Red de Expertos. Se identifican los cambios en negrita y cursiva.	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Claudio Paredes/ Jefe de Ingeniería y Explotación de Sistemas DINFO; Ivonne Valdivia / Profesional Depto. Estudios DIVAD; Marcela Jara/ Analista Dpto. de Planificación y Control de Gestión DIFIN; M. Paula Melis Otonel/ Contralora Interna SERVIU Araucanía.

Revisión:	Guillermo Rolando Vicente/ Subsecretario de Vivienda y Urbanismo. Marcela Acuña Gómez/ Jefa Gabinete Subsecretaría – Encargada de Seguridad de la Información. Andrea Ubal Espinoza / Jefe Sección Control de Gestión DIFIN. Comité de Seguridad de la Información Subsecretaría de V. y U. Encargados/as de Seguridad de la Información de SERVIU y Parque Metropolitano.
Aprobación:	Cristián Monckeberg Bruner / Ministro de Vivienda y Urbanismo.

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA
ABOGADA
DIVISIÓN JURÍDICA