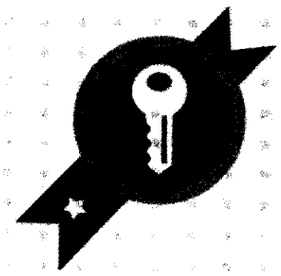
Ministerio de Vivienda y Urbanismo

Gobierno de Chile

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN



MINISTERIO DE VIVIENDA Y URBANISMO

VERSIÓN 06

MINISTERIO DE VIVIENDA Y URBANISMO
M. CECILIA CACERES
Jefa
DIVISIÓN JURÍDICA

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

CONTENIDO

0. GLOSARIO

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.
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 sirven para los propósitos de la Institución.
Seguridad de la Información	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.
Confidencialidad	La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren
Integridad	La propiedad de salvaguardar la exactitud y completitud de los activos.
Documento de Aplicabilidad	Declaración documentada que describe los controles que son relevantes para el SGSI de la organización y aplicables al mismo, así como el rol de cada institución del MINVU en la implementación de los controles de la norma ISO 27001:2013.

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

MINISTERIO DE VIVIENDA Y URBANISMO
M. CECILIA CACERES
Jefa
DIVISIÓN JURÍDICA

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

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 vivienda, barrio y ciudad".*

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 en 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[1].

2. 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 [2], 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.

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

La presente política es aplicable a funcionarios de planta, contrata y honorarios que forman parte del Ministerio de Vivienda y Urbanismo (Subsecretaría de Vivienda y Urbanismo (Nivel central y 15 SEREMI), 15 SERVIU y Parque Metropolitano de Santiago), así como también a asesores, consultores, practicantes y personas naturales o jurídicas que prestan servicios para el MINVU.
Sin perjuicio de lo anterior, cada Servicio[3] puede definir las políticas específicas de Seguridad de la Información que considere necesarias y que son de aplicación local, sin embargo, éstas no pueden contener elementos que contravengan la presente política, aplicándose además esta última en todos los aspectos no regulados por aquellas.

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.***

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

[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.

[3] El término "Servicio" hace referencia a Subsecretaría de Vivienda y Urbanismo (Nivel central y 15 SEREMI), 15 SERVIU y Parque Metropolitano de Santiago

MINISTERIO DE VIVIENDA Y URBANISMO
M. PAZ VILLA CACERES
Jefa
DIVISIÓN JURÍDICA

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. ***Política de Seguridad de la Información***
2. ***Organización de la Seguridad de la Información***
3. ***Seguridad de los Recursos Humanos***
4. ***Gestión 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 de los Sistemas de Información***
11. ***Relaciones con el proveedor***
12. ***Gestión de Incidentes en la Seguridad de la Información***
13. ***Aspectos de la Seguridad de la Información el a gestión de la continuidad del negocio***
14. ***Cumplimiento***

Para todos estos dominios, se establecerán 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 todos los funcionarios en la intranet institucional.

La definición de los procesos (asociados a los productos estratégicos[4]), que forman parte del SSI, ***es*** formalizado por cada Servicio, a través de un documento que contiene los fundamentos y criterios de dicha selección.

Cabe destacar que independiente del Alcance definido en cada Servicio, existen algunos controles normativos que son de aplicación transversal a toda la institución.

Adicionalmente, se cuenta con el "Documento de Aplicabilidad", en el cuál se identifican los controles de la norma ISO 27001:2013, su aplicabilidad institucional y el rol de Subsecretaría, SERVIU y PMS en su implementación.

4. ROLES Y RESPONSABILIDADES

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

⇨ Un/a 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 de este sistema de gestión y la satisfacción de las partes interesadas.

⇨ Un 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.

[4] Los productos estratégicos se encuentran definidos en el Formulario de Definiciones Estratégicas (Formulario A1) vigente de los correspondientes Servicios, disponible en http://www.dipres.gob.cl/595/w3-propertyvalue-15400.html. Los procesos asociados a productos también se les denomina "procesos de provisión de bienes y servicios", o "del negocio".

MINISTERIO DE VIVIENDA Y URBANISMO CECILIA CACERES Jefa DIVISIÓN JURÍDICA

MINISTERIO DE VIVIENDA Y URBANISMO JUAN PABLO RÍOS Abogado DIVISIÓN JURÍDICA

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, tienen como responsabilidades cumplir las políticas de seguridad de la información del MINVU, asegurar la confiabilidad, disponibilidad e integridad de la información que tienen a su cargo y reportar oportunamente los incidentes de seguridad de la información que detecte.

5. DISPOSICIONES PARA RESGUARDAR LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la 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 LA 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 preservan el principio de transparencia de la función pública[5] recogido en la Ley 20.285 sobre Acceso a la Información Pública.

Por lo anterior, y dada la condición pública de la información elaborada con presupuesto público 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 20.285.

Además, el resguardo de la información involucra la obligación de las personas que trabajan en el tratamiento de datos personales o tengan acceso a estos, de guardar secreto sobre los mismos, según Ley 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 LA INFORMACIÓN

El MINVU ***establece*** lineamientos, prácticas de seguridad y mecanismos que aseguran la integridad de la 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 LA INFORMACIÓN

EL MINVU ***asegura*** la disponibilidad de la 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 a pérdida la información relevante y que mantengan la continuidad del flujo de información.

6 GESTIÓN DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

6.1 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

MINISTERIO DE VIVIENDA Y URBANISMO
M. CECILIA CACERES
Jefa
DIVISIÓN JURÍDICA

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

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

propósito. Asimismo, para la implementación operativa de algunas políticas específicas de seguridad, se ***elaboran*** procedimientos u otros documentos que se alinean con los parámetros establecidos de documentación en cada Servicio.

6.2 APROBACIÓN DE UNA POLÍTICA Y OTROS DOCUMENTOS

Las políticas específicas de seguridad ***son*** aprobadas por el Jefe de Servicio, y los procedimientos por los Jefes/Encargados de cada área respectiva o el Encargado de Seguridad de la Información de cada Servicio ***o el Jefe de Servicio,*** dependiendo de los lineamientos y prácticas de seguridad particulares o transversales, conforme a su estructura y requerimientos de seguridad. ***Dicha aprobación se formaliza a través de correo electrónico, acta de reunión del comité de seguridad de la información, acto administrativo emitido por el Jefe de Servicio u otro mecanismo que se establezca para tal efecto.***

6.3 PUBLICACIÓN Y COMUNICACIÓN 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 todos los funcionarios puedan acceder a la documentación.***

La comunicación de la presente política, las políticas específicas de seguridad, los procedimientos y otros documentos, se ***efectúa*** de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, pudiendo utilizarse los canales de difusión establecidos, como Intranet, Minvuletín, ***correo electrónico,*** entre otros.

6.4 REVISIÓN DE LA POLÍTICA

La presente política será revisada anualmente o cuando el MINVU 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 al ambiente técnico, recomendaciones realizadas por autoridades pertinentes, tendencias relacionadas con amenazas y las 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.

7 SANCIONES APLICABLES

El incumplimiento o violación a esta política, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, ***para*** los funcionarios del MINVU, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

MINISTERIO DE VIVIENDA Y URBANISMO
M. CECILIA CACERES
Jefa
DIVISIÓN JURÍDICA

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

CONTROL DE VERSIONES

Versión	Fecha Aprob.	Motivo de la revisión	Autor(es)
05	Nov. 2015	Actualización norma ISO 27001 y cambio de versión	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Ivonne Valdivia / Profesional Depto. Estudios DIVAD; Miguel Ancamil Ramos / Profesional Depto. Estudios DIVAD; Juan Pablo Ríos / Abogado DIJUR; María Waleska Gatica Norambuena / Abogado DIJUR; Marcela Jara Cartes / Analista Sección Gestión de Procesos DIFIN; Paulo Torreblanca / Analista Sección Gestión de Procesos DIFIN; Gonzalo Fernández Rodríguez / Enc. Sección Gestión de Procesos DIFIN.
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.

Revisión:	Iván Leonhardt Cárdenas / Subsecretario de Vivienda y Urbanismo. Alexia Naranjo Loyola / Encargada de Seguridad de la Información. Andrea Ubal Espinoza / Jefa (S) Depto. Planificación y 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:	Paulina Saball Astaburuaga / Ministra de Vivienda y Urbanismo.

MINISTERIO DE VIVIENDA Y URBANISMO
M. CECILIA CACERES Vera
DIVISIÓN JURÍDICA

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA