Ministerio de Vivienda y Urbanismo

Gobierno de Chile

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE VIVIENDA Y URBANISMO

VERSIÓN 5

Nota: Versión para impresión y difusión en formato carta, de la Resolución N° 9103 del 23/11/2015 de Ministra de Vivienda y Urbanismo.

CONTROL DE VERSIONES

Versión	Fecha Aprob.	Motivo de la revisión	Autor(es)
4	Dic. 2012	Correcciones de contenido	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Claudio Paredes/ Jefe de Ingeniería y Explotación de Sistemas DINFO; Claudia Elgueta/ Profesional Depto. Planificación y Control de Gestión DIFIN; Marcela Jara/ Profesional Depto. Planificación y Control de Gestión DIFIN; Ximena Gutiérrez/ Enc. Sección Procesos, Depto. Planificación y Control de Gestión DIFIN; Carlos Pinto / Abogado DIJUR
5	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.

Revisión:	Vania Navarro Morales / Jefa Depto. Planificación y Control de Gestión DIFIN. Encargados/as de Seguridad de la Información de SERVIU y Parque Metropolitano. Héctor Opazo Díaz / Encargado de Seguridad de la Información. Jaime Romero Álvarez / Subsecretario de Vivienda y Urbanismo.
Aprobación:	Paulina Saball Astaburuaga / Ministra de Vivienda y Urbanismo.

CONTENIDO

1. DECLARACIÓN INSTITUCIONAL

El Ministerio de Vivienda y Urbanismo –MINVU– ha decidido establecer, implementar, mantener y mejorar continuamente Sistemas 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, tal 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 ajustarán 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

La gestión de seguridad de la información en el MINVU tiene como principales objetivos:

- ⇨ 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 operacional a través de acciones tendientes a gestionar los incidentes y a revertir y resolver contingencias[2] que se detecten.

Para lo anterior, en el marco del SSI, se desplegará un conjunto de lineamientos y prácticas de seguridad de la información –en consistencia con las disposiciones indicadas en esta política en los puntos 5 y 6– debiendo ser formalizadas a través de políticas específicas, procedimientos y otros documentos para su cumplimiento y aplicación por parte de las personas, especialmente en 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 formen parte del Ministerio de Vivienda y Urbanismo (Subsecretaría de Vivienda y Urbanismo, 15 SEREMI, 15 SERVIU y Parque Metropolitano de Santiago), así como también a asesores, consultores, practicantes y personas naturales o jurídicas que presten servicios para el MINVU.

Sin perjuicio de lo anterior cada Servicio, puede definir las políticas específicas de Seguridad de la Información que considere necesarias, y que serán de aplicación local, sin embargo, no pueden contener elementos que contravengan la presente política, aplicándose además esta última en todos los aspectos no regulados por aquellas.

[1] Disponible en www.minvu.cl, enlace "Marco Normativo".
[2] Las contingencias pueden ser menores y mayores, dependiendo del grado y alcance de sus consecuencias a nivel organizacional.

Las copias impresas de este documento corresponden a versiones no controladas.

Para el desarrollo del SSI, se consideran los requisitos de la norma NCh-ISO 27001:2013, desplegando las buenas prácticas según orientaciones indicadas en la NCh-ISO 27002:2013.

La definición de los procesos (asociados a los productos estratégicos[3]), que forman parte del SSI, será formalizado por cada servicio, a través de un documento que contenga los fundamentos y criterios de dicha selección.
Cabe destacar que independiente del Alcance definido en cada Servicio, existen algunas prácticas que son de aplicación transversal a toda la institución.

4. ROLES Y RESPONSABILIDADES

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

- Un/a Encargado/a de Seguridad de la Información, en cuyo rol el Jefe de Servicio delega las decisiones relativas a la seguridad de la información institucional 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 que tiene injerencia en las decisiones estratégicas relativas a la seguridad de la información, a partir de los dominios que regulan los diferentes aspectos.

- La designación de uno o más responsables del reporte, registro, solución y escalamiento de incidentes de seguridad de la información que se detecten a nivel institucional o ministerial.

- La nominación de uno o más responsables de la coordinación ante contingencias que afecten la continuidad de las operaciones.

[3] Los productos estratégicos se encuentran definidos en el Formulario de Definiciones Estratégicas 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”.

Las copias impresas de este documento corresponden a versiones no controladas.

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 abordará estos principios básicos de Seguridad de la Información.

5.1 DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

El MINVU se comprometerá a resguardar 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[4] 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 obre 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 éstos de otra forma- de guardar secreto sobre los mismos, según Ley 19.628 de Protección de Datos de Carácter Personal.

De este modo, cada Servicio se comprometerá a implementar los controles necesarios para garantizar que tanto la información física como 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 se comprometerá a preservar la integridad de la información institucional, asegurando la máxima factibilidad que esta sea mantenida con exactitud tal cual fue generada, trasportada o trasmitida, sin ser manipulada o alterada por personas o procesos no autorizados. Para ello, se establecerán lineamientos, prácticas de seguridad y mecanismos que aseguren 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 asegurará la disponibilidad de la información institucional, 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.

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

Las copias impresas de este documento corresponden a versiones no controladas.

6 DISPOSICIONES PARA ASEGURAR LA CONTINUIDAD DE LAS OPERACIONES

Las actividades en procesos, y los activos de información que contienen, se encuentran expuestos a incidentes que pueden derivar en contingencias en las operaciones de cada Servicio o SEREMI. El SSI propicia disminuir la probabilidad de ocurrencia y las consecuencias negativas de estos sucesos, mediante lineamientos y la aplicación de prácticas de seguridad tendientes a su gestión y efectiva solución.

6.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El MINVU definirá lineamientos a través de una política específica y describirá las prácticas de gestión de incidentes de seguridad de la información, mediante procedimientos que aborden a nivel institucional y/o ministerial, los tipos de incidentes que corresponda.

La gestión de incidentes de seguridad de la información contemplará actividades claves, tales como: la detección, registro y reporte a áreas pertinentes de un incidente de seguridad de la información, su análisis (considerando su priorización, su declaración como incidente y descarte), su pronta solución, su escalamiento a autoridades internas como externas, su respuesta y seguimiento, además de la recopilación y preservación de evidencias.

6.2 GESTIÓN DE LA CONTINUIDAD ANTE CONTINGENCIAS

El MINVU establecerá lineamientos a través de una política específica y determinará las prácticas de gestión de continuidad de las operaciones[5], mediante uno o más de planes de contingencia o continuidad a nivel institucional y/o ministerial, en los niveles que corresponda.

La gestión de continuidad de las operaciones considerará aspectos claves, tales como: la definición de una estructura organizacional adecuada para resolver acciones en cada plan; la determinación de escenarios posibles; un análisis de riesgos y consecuencias asociadas a dichos escenarios; las estrategias de continuidad de los procesos; el desarrollo de procedimientos alternativos de operación, si corresponde; los componentes informáticos y no informáticos de apoyo y las acciones de recuperación ante contingencias.

[5] Asimilación en el MINVU del concepto “continuidad del negocio”, indicado en la norma NCh-ISO 27001:2013.

Las copias impresas de este documento corresponden a versiones no controladas.

7 GESTIÓN DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

7.1 GENERACIÓN DE UNA POLÍTICA Y OTROS DOCUMENTOS

Para el desarrollo de las políticas de seguridad se adoptará un formato especificado para el SSI, ciñéndose a pautas convenidas con los actores que tengan injerencia en el despliegue de este sistema de gestión en cada Institución.

Asimismo, para la implementación operativa de algunas políticas específicas de seguridad se elaborarán procedimientos u otros documentos que se alineen a parámetros establecidos de documentación en cada Servicio.

7.2 APROBACIÓN DE UNA POLÍTICA Y OTROS DOCUMENTOS

Las políticas específicas de seguridad serán aprobadas por el Jefe de Servicio, y los procedimientos serán aprobados por los Jefes/Encargados de cada área respectiva o del Encargado de Seguridad de la Información de cada Servicio, dependiendo de los lineamientos y prácticas de seguridad particulares o transversales, conforme a su estructura y requerimientos de seguridad.

7.3 PUBLICACIÓN Y COMUNICACIÓN DE UNA POLÍTICA Y OTROS DOCUMENTOS

Las versiones vigentes de la presente política y toda documentación vinculada al Sistema de Seguridad de Información serán publicadas en el sitio web de cada Institución, además de otros lugares visibles disponibles.

La comunicación de la presente política, las políticas específicas de seguridad, los procedimientos y otros documentos se efectuará 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, entre otros.

7.4 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, mendiante auditorías internas, externas y/o revisiones independientes.

8 SANCIONES APLICABLES

El incumplimiento o violación a esta política, debidamente acreditado, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a 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.

Las copias impresas de este documento corresponden a versiones no controladas.