Ministerio de Vivienda y Urbanismo

Gobierno de Chile

APRUEBA POLÍTICA ESPECÍFICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, EN EL MARCO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO.

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA
20 DIC 2019
RESOLUCION EXENTA
TRAMITADA

20 DIC 2019

SANTIAGO, HOY SE RESOLVIO LO QUE SIGUE

RESOLUCIÓN EXENTA Nº 2954

VISTO: Lo dispuesto en el D.L Nº 1305, de 1975, que reestructura y regionaliza el Ministerio de Vivienda y Urbanismo; en el D.S Nº 83, de 2004, de MINSEGPRES, que aprueba norma técnica para los órganos de la administración del Estado sobre la seguridad y confidencialidad de los documentos electrónicos; la norma chilena NCh-ISO 27001:2013, sobre Sistema de Gestión de Seguridad de la Información - requisitos; la Resolución Exenta Nº 2.097, (V. y U.), de 2019, que aprueba la Política General de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo el Instructivo Presidencial Nº 08/2018, que imparte instrucciones urgentes en materias de Ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado, la Resolución Nº 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 se han dictado una serie de normas entre las que se encuentra el Decreto Supremo Nº 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, y las Normas Chilenas NCh-ISO 27001:2013 que proporciona un marco de gestión de Seguridad de la Información utilizable por cualquier tipo de organización, pública o privada.

b. Que, mediante la Resolución Exenta Nº 2.097, (V. y U.), de 2019, se ha aprobado una nueva Política General de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo, sus 16 Servicios de Vivienda y Urbanización, el Parque Metropolitano de Santiago y la Subsecretaría de Vivienda y Urbanismo (Nivel Central y sus 16 Secretarías Regionales Ministeriales).

c. Que no obstante lo anterior, resulta necesario establecer Políticas Específicas de seguridad de la información para materializar de una manera más efectiva la Política General anteriormente citada, por lo que dicto la siguiente

RESOLUCIÓN:

I. **Apruébese** la Política Específica de Gestión de Incidentes de Seguridad de la Información.

MINISTERIO DE VIVIENDA Y URBANISMO
DIVJ
JUF

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

"POLÍTICA ESPECÍFICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN"

1. OBJETIVO

Esta política establece las responsabilidades y procedimientos para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

2. ALCANCE

La presente Política considerada como parte del Dominio de Gestión de Incidentes de Seguridad de la Información, en particular al control A.16.01.01 Responsabilidades y procedimientos de la norma NCh ISO 27001:2013, es aplicable ante la ocurrencia de incidentes de seguridad de la información que puedan comprometer las operaciones y amenazar la confidencialidad, integridad y/o disponibilidad de los activos de información.

Esta Política debe ser cumplida por todos los usuarios de la Subsecretaría de Vivienda y Urbanismo, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presten servicios al MINVU.

Los Servicios de Vivienda y Urbanización y el Parque Metropolitano de Santiago, en uso de las facultades que le son propias podrán acogerse a esta Política, para lo cual deberán dictar el respectivo acto administrativo que dé cuenta de ello.

3. NOMENCLATURA

MAU: Mesa de Ayuda

SERVIU: Servicios de Vivienda y Urbanización

PMS: Parque Metropolitano de Santiago

4. DOCUMENTOS RELACIONADOS.

- Decreto Supremo N° 83, de 2004, Norma Técnica para los Órganos de la administración del Estado sobre seguridad y confidencialidad.
- Norma Chilena ISO 27001:2013.
- Política General de Seguridad de la Información.
- Procedimiento de Gestión de Incidentes de Seguridad de la Información.

5. ROLES Y RESPONSABILIDADES.

Encargado/a de Seguridad de la Información.

- Apoyar en el desarrollo e implementación de los procedimientos de respuesta ante incidentes.
- Participar en la evaluación y respuesta a incidentes de seguridad.
- Velar por el cumplimiento de esta Política.

Encargados de áreas/servicios - MAU

- Recibir información de eventos e incidentes de seguridad.
- Registrar reporte de incidente de seguridad.
- Gestionar con unidades resolutoras TI.
- Informar al SIRT de los incidentes de seguridad.
- Reportar los incidentes de seguridad.

Equipo de respuesta ante incidentes de seguridad de la información - SIRT.

- Promover el desarrollo de procedimientos de respuesta a los incidentes de seguridad de la información.
- Establecer lazos institucionales y de coordinación que permitan hacer preparativos para una adecuada respuesta a incidentes de seguridad de la información.
- Registrar todo incidente de seguridad de la información reportado.
- Difundir y sensibilizar los incidentes ocurridos.

Personal MINVU

- Reportar todo evento, debilidad y/o incidente de seguridad de la información que sea detectado o conocido, tan pronto sea posible, utilizando los canales de comunicación establecidos.

Jefe/a Superior de Servicio

- Recibir y coordinar la respuesta y/o solución en casos de incidentes de seguridad críticos y/o sensibles y reportar al Encargado/a de Seguridad de la Información en caso de que sea considerado un incidente de seguridad de la información.
- Definir acciones adicionales para aquellos incidentes que hayan sido escalados por el Comité SSI.

6. REGLAS DE LA POLÍTICA

6.1 Definición de incidente de seguridad de la información.

Corresponde a una serie de sucesos adversos, tales como:

- Uno o más eventos indeseados o inesperados que impacten la confidencialidad; integridad o disponibilidad (continuidad) de activos de información, informáticos o no informáticos, asociados a los procesos institucionales.
- El incumplimiento de cualquier Política de seguridad de la información de la institución.
- Todo evento expresamente tipificado en el MINVU como incidente de seguridad de la información.

6.2 Equipo de respuestas ante incidentes de seguridad - SIRT.

Deberá existir un equipo de funcionarios responsables y entrenados para el manejo de incidentes de seguridad de la información, a objeto de elaborar y promover los procedimientos respectivos a la respuesta de aquéllos.

Este equipo de personas deberá estar compuesto por representantes de los distintos Servicios y áreas del MINVU, que permitan un necesario consenso y un nivel de toma de decisiones adecuado.

En la Subsecretaría de Vivienda y Urbanismo, estas áreas corresponden al:

- Gabinete Subsecretario/a de Vivienda y Urbanismo
- División Informática
- División Administrativa
- División de Finanzas
- División Jurídica
- Cualquier otra División o unidad ministerial que forme parte de los procesos en alcance del Sistema de Seguridad de la Información -SSI.

En los respectivos Servicios y/o SEREMI, estas áreas corresponderán a:

- Los Departamentos de Administración y/o Finanzas.
- Departamentos o áreas jurídicas.
- Las unidades asesoras en materia de control de gestión.
- Cualquier área o unidad que forme parte de los procesos en alcance del Sistema de Seguridad de la Información -SSI.

Este equipo es responsable de establecer lazos institucionales y de coordinación que permitan hacer preparativos para respuesta ante incidentes, con las entidades externas que se listan a continuación:

- Equipos de seguridad de los proveedores de hardware y software.
- Especialistas en delitos computacionales.
- Asesoría legal en delitos computacionales.
- Policía
- Bomberos
- Servicios médicos.

6.3 Procedimientos para incidentes conocidos.

El equipo de respuestas ante incidentes de seguridad - SIRT- debe definir al menos un procedimiento global para incidentes informáticos e incidentes no informáticos, que señale las principales actividades a desarrollar para una adecuada respuesta a los incidentes.

Debe existir un diccionario de eventuales incidentes de seguridad de la información, sean estos informáticos o no informáticos, distinguiendo también aquellos eventos que no forman parte de éstos. Este diccionario debe formar parte de los antecedentes para la distinción y evaluación del incidente de seguridad reportado.

6.4 Registro y solución del incidente.

Cada incidente de seguridad debe ser reportado, investigado y registrado.

El Equipo de respuesta ante incidentes de seguridad -SIRT- debe mantener registro de los incidentes reportados y su seguimiento.

6.5 Actividades generales a considerar frente a cualquier tipo de incidente.

- Se debe mantener un registro de los incidentes reportados y su seguimiento.
- Las actividades generales que deben ser consideradas como parte del proceso de gestión de un incidente, deben considerar:
  - Identificación del tipo de incidente.
  - Evaluación de impacto.
  - Activación de las notificaciones adecuadas.
  - Escalamiento del incidente, dependiendo de su gravedad y permanencia en el tiempo.
  - Identificación de contactos internos y/o externos previamente definidos
  - Identificación y ejecución de las actividades o procedimientos que apliquen.
  - Seguimiento a la evolución del mismo
  - Informe a la jefatura respectiva.
- Una vez superado el incidente, se debe analizar las acciones tomadas, además de evaluar la consistencia de las políticas, procedimientos y otros documentos que se hayan utilizado para tal efecto.

6.6 Revisión de acciones reportadas.

- El conocimiento y solución de un incidente de seguridad, debe generar acciones correctivas, preventivas y proposiciones de mejora.
- De acuerdo con la gravedad del incidente de seguridad, podría originar una medida disciplinaria.
- Una vez superado el incidente, analizar las acciones tomadas y evaluar la consistencia de las políticas y procedimientos utilizados.

- Se deben efectuar actividades de revisión de incidentes repetitivos, los que deben necesariamente generar la activación de resolución de problemas.

7. DIFUSIÓN

La comunicación y difusión de la presente política específica es responsabilidad del Encargado de Seguridad de la Información o en quien designe esta función, pudiendo utilizar para ello los canales de difusión establecidos, como 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.

Adicionalmente, las Políticas específicas se encuentran publicadas en la página web del MINVU en la sección MINVU/ Políticas de Seguridad de la Información.

8. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

La presente política específica debe ser revisada anualmente, o cuando el Servicio 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, el Servicio evaluará el cumplimiento de la presente política, a lo menos cada tres años, mediante auditorías internas, externas y/o revisiones independientes.

9. CONTROL DE VERSIONES

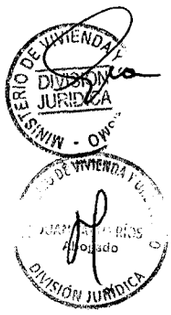
Nº Versión	Fecha Aprobación	Motivo de la revisión
01	Diciembre 2019	Versión inicial

Elaborado por:

Leonardo Cavieres Córdoba/ Encargado de Seguridad Informática, División de Informática; Claudio Paredes Pizarro/ Encargado de Sección de Ingeniería y Explotación de Sistemas, División de Informática; Juan Pablo Ríos/ Abogado, División Jurídica; Ivonne Valdivia Galindo/Analista Depto. de Estudios, División Administrativa; Marcela Jara Cartes/ Analista Depto. Planificación y Control de Gestión, División Finanzas.

Revisado por:

Marcela Acuña Gómez, Encargada de Seguridad de la Información; Agustín Goñi Gonzalez, Jefe División de Informática; Claudia Ernst Valencia, Jefe División Administrativa, Claudia Hidalgo Pérez, Asesora Subsecretaría de Vivienda y Urbanismo; Andrea Ubal Espinoza/Jefa de Control de Gestión, División de Finanzas



II. **Difúndase** la Política fijada por este instrumento por el Encargado/a de Seguridad de la Información de la Subsecretaría de Vivienda y Urbanismo y, en coordinación con el Comité de Seguridad de la Información velar por su estricto cumplimiento.

III. **Realícense** por el/la Encargado/a de Seguridad de la Información de la Subsecretaría de Vivienda y Urbanismo las acciones tendientes a su implementación en materias de su competencia.

IV. La presente resolución no irroga gastos para el presupuesto de este Ministerio.

ANÓTESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIO

GUILLERMO ROLANDO VICENTE
SUBSECRETARIO DE VIVIENDA Y URBANISMO

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

PABLO ZAMBRANO TORQUERA
INGENIERO DE EJECUCIÓN
MINISTRO DE FE
MINISTERIO DE VIVIENDA Y URBANISMO

MAG/AGG/CEV/GEA/ACA/AUE

DISTRIBUCIÓN:

- Gabinete Ministro V. y U.
- Gabinete Subsecretario V. y U.
- SEREMI (16)
- SERVIU (16)
- PMS
- Divisiones Nivel Central (7)
- Auditoría Interna Ministerial
- Contraloría Interna Ministerial
- Comisión Asesora para la Reducción de Riesgo de Desastres y Reconstrucción
- Sistema Integrado de Atención a la Ciudadanía (SIAC)
- Depto. Comunicaciones
- Comisión de Estudios Habitacionales y Urbanos (CEHU)
- Depto. Planificación y Control de Gestión DIFIN
- Oficina de Partes
- Ley de Transparencia Art. 7/g

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA