Ministerio de Vivienda y Urbanismo

Gobierno de Chile

APRUEBA PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN V06 PARA LA SUBSECRETARÍA DE VIVIENDA Y URBANISMO (NIVEL CENTRAL Y SUS 16 SECRETARIAS REGIONALES MINISTERIALES).

30 OCT 2019

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA
30 OCT 2019
RESOLUCIÓN TRAMITADA

SANTIAGO, **2452**

RESOLUCIÓN EXENTA N° _____/

HOY SE RESOLVIO LO QUE SIGUE

VISTOS: Lo dispuesto en el D.L N° 1.305, de 1975, que Reestructura y Regionaliza el Ministerio de Vivienda y Urbanismo; en el D.S N° 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 N° 2.097, (V. y U.), de 2019, que aprueba la Política General de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo; 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 se han dictado una serie de normas en materia de seguridad de la información, entre las que se encuentra el Decreto Supremo N° 83, de 2004, 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; la Norma Chilena NCh-ISO 27001:2013, que proporciona un marco de gestión de Seguridad de la Información utilizable por cualquier tipo de organización, pública o privada y el Instructivo Presidencial N° 008 de 2018, que imparte instrucciones en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los Órganos de la Administración del Estado.

b) Que resulta necesario establecer procedimientos que entreguen lineamientos operativos para la implementación del sistema de seguridad de la información.

RESOLUCIÓN:

I. **Apruébase** el Procedimiento de Gestión de Incidentes de Seguridad de la Información, versión 06.

1 OBJETIVO

Este documento establece las medidas para detectar, reportar, evaluar y gestionar los incidentes de seguridad de la información, tanto de carácter informáticos (incluye ciberseguridad) como no informáticos que comprometan la seguridad de los Activos de Información de la institución y mejorar continuamente la gestión de incidentes.

2 ALCANCE

Este documento es aplicable a funcionarios de planta, contrata y honorarios que formen parte del Ministerio de Vivienda y Urbanismo (Subsecretaría de Vivienda y Urbanismo, 16 SEREMI, 16 SERVIU y Parque Metropolitano de Santiago), así como también a asesores, consultores, practicantes, personas naturales o jurídicas que presten servicios para el MINVU.

Este procedimiento está relacionado con el cumplimiento de los controles 16.01.01, 16.01.02, 16.01.03, 16.01.04, 16.01.05, 16.01.06 y 16.01.07 de la norma NCh ISO 27001:2013.

3 SIGLAS Y DEFINICIONES

SSI	Sistema de Seguridad de la Información
MAU	Mesa de Atención al Usuario
PMS	Parque Metropolitano de Santiago
SERVIU	Servicio de Vivienda y Urbanización
CSIRT	Computer Security Incident Response Team - CSIRT- (Equipo de Respuesta ante Incidentes de Seguridad de la Información). La denominación de CSIRT corresponde al actual equipo de seguridad de la Red de Conectividad del Estado de la Subsecretaría del Interior.
Evento de seguridad de la información	Suceso que indica una posible brecha en la seguridad de la información o falla en el control de ésta.
Incidente de seguridad de la información	Corresponde a uno o varios eventos identificados que cumplen una serie de criterios establecidos y que puedan dañar los activos de una organización o comprometer sus operaciones.
Sistema Aranda	Aranda Service Desk es una herramienta que permite gestionar diferentes procesos del negocio a través de una misma consola y dar soporte a diferentes tipos de casos como: Solicitudes, requerimientos de servicio, eventos, problemas y cambios. Ofrece versatilidad para el registro y seguimiento de casos por parte del cliente, a través de la plataforma web de usuario final, permitiendo la autogestión de casos con la base de conocimientos o el registro de una nueva solicitud en la Mesa de Servicio.

Gestiona.MINVU	Sistema en el cual se registran los incidentes de seguridad de la información, se definen acciones para abordarlos, se registra la implementación de las acciones y se evalúa su eficacia.

4 ROLES Y RESPONSABILIDADES [1] (A.16.01.01)

Se describen los principales actores identificados en el proceso:

Rol/Actor	Responsabilidad general en el procedimiento
Personal MINVU, asesores, consultores, practicantes, personas naturales o jurídicas que presten servicios para el MINVU	- Son quienes usan, manipulan o poseen activos de información a partir de los cuáles detectan y reportan eventos o debilidades en la seguridad de la información.
Analista MAU	- Recibe, registra, evalúa y coordina acciones para abordar **eventos o debilidades de tipo informático** en **Nivel Central**. - Clasifica los eventos o debilidades como incidente de seguridad de la información informático en Nivel Central y los reporta al Encargado de Gestión de Incidentes de la DINFO.
Equipo DIVAD	- Reciben y coordinan acciones para abordar **eventos o debilidades de tipo no informático** en **Nivel Central.** - Revisan y evalúan si los eventos o debilidades reportadas de tipo no informático, corresponden a un incidente de seguridad de la información y los reportan al Encargado de Gestión de Incidentes de la DIVAD.
Coordinador Informático o Encargado Sección Informática SEREMI, SERVIU y PMS	- Recibe, registra, evalúa y coordina acciones para abordar **eventos o debilidades de tipo informático** en **Seremi, Serviu y PMS**. - Clasifica los eventos o debilidades como incidente de seguridad de la información informático y los reporta al Encargado de Gestión de Incidentes del Servicio.
Coordinador Área de Administración SEREMI, SERVIU y PMS	- Recibe, registra, evalúa y coordina acciones para abordar **eventos o debilidades de tipo no informático** en **Seremi, Serviu y PMS**. - Evalúa si los eventos o debilidades corresponden a un incidente de seguridad de la información no informático y los reportan al Encargado de Gestión de Incidentes del Servicio.

[1] El uso de un lenguaje que no discrimine ni marque diferencias de género es una de las preocupaciones de nuestra Institución. En tal sentido y con el fin de evitar la sobrecarga gráfica que supondría utilizar en español "o/a" para marcar la existencia de ambos sexos, hemos optado por emplear el masculino genérico clásico, en el entendido que todas las menciones en tal género representan siempre a hombres y mujeres.

Rol/Actor	Responsabilidad general en el procedimiento
Contraparte Técnica Proveedores	- Recibe información sobre eventos o debilidades de seguridad de la información y reporta de acuerdo a la clasificación de tipo de evento o debilidad.
Encargado de Gestión de Incidentes	- Es el responsable de coordinar la respuesta y /o solución en casos de incidentes de seguridad de la información y de dejar registro de ello en el Sistema Gestiona MINVU.
Encargado de Seguridad Informática del MINVU	- Gestiona incidentes informáticos y coordina la obtención de su respuesta. - Asesora en la clasificación de eventos o debilidades como incidentes de seguridad de la información de tipo informático. - Encargado de Gestión de Incidentes de tipo informático en Nivel Central.
Encargado de Seguridad de la Información	- Registra los **incidentes de seguridad de la información de tipo sensible** o escalados al Jefe de Servicio y coordina la respuesta y/o solución, dejando registro en el Sistema Gestiona MINVU. - Es el canal de comunicación hacia el CSIRT de Gobierno. - Definen la responsabilidad de evaluar la eficacia de los planes de acción.
Coordinador DIVAD	- Asume el rol de Encargado de Gestión de Incidentes de tipo no informático en Nivel Central.
Jefe de Servicio	- Recibe y coordina la respuesta y/o solución en casos de incidentes de seguridad críticos y/o sensibles y reporta al Encargado de Seguridad de la Información en caso de que sea considerado un incidente de seguridad de la información. Además de definir acciones adicionales para aquellos incidentes que hayan sido escalados por el Comité SSI.
Comité de SSI	- Evalúa acciones a tomar para los incidentes no eficaces y escala incidentes declarados no eficaces cuando lo considere pertinente. - Revisa periódicamente el estado de los incidentes de seguridad de la información y anualmente el Informe de Aprendizaje de Gestión de Incidentes de Seguridad de la Información.
Equipo de Investigación de Incidentes	- Apoyar en la investigación de los incidentes de seguridad de la información, recolectando la mayor cantidad de información que permita tener claridad absoluta respecto al incidente.
Coordinador Nacional de Seguridad de la Información y Ciberseguridad	- Genera, consolida y envía el Informe de Aprendizaje de Gestión de Incidentes de Seguridad de la Información, además de calcular y hacer seguimiento al indicador del proceso de Gestión de Incidentes de Nivel Central.

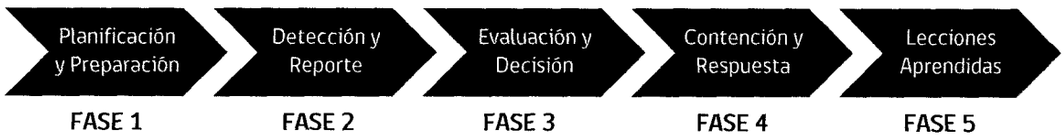
5 DESCRIPCIÓN

Un evento de seguridad de la información es un suceso que indica una posible brecha en la seguridad de la información o falla en el control de ésta. Un incidente de seguridad de la información corresponde a uno o varios eventos identificados que cumplen una serie de criterios establecidos y que puedan dañar los activos de una organización o comprometer sus operaciones.

Un evento de seguridad de la información no significa necesariamente que un ataque ha sido exitoso o que se hayan visto afectadas la confidencialidad, integridad o disponibilidad, por nombrar algunos ejemplos. Es decir, no todos los eventos de seguridad de la información son clasificados como incidentes de seguridad.

Los incidentes de seguridad de la información pueden ser deliberados (por ejemplo, causados por un software malicioso o una falta disciplinaria intencional) o accidentales (por ejemplo, un error humano involuntario o por actos inevitables de la naturaleza) y pueden ser causados por medios técnicos (por ejemplo, virus computacional) o no técnicos (pérdida o robo de un computador). Las consecuencias pueden incluir la divulgación no autorizada, modificación, destrucción, la inaccesibilidad de información, o daño o robo de activos de la organización que contengan información.

Con el fin de evitar o contener el impacto de un incidente de seguridad de la información y así minimizar el daño directo o indirecto a sus operaciones, la Subsecretaría de Vivienda y Urbanismo, de acuerdo a lo establecido en la Política Específica de Gestión de Incidentes de SI, ha definido un enfoque estructurado y planificado para la gestión de incidentes de seguridad de la información, definiendo las siguientes fases para abordarlos:



Adicionalmente se han definido contrapartes tanto a Nivel Central como regional para que actúen como Encargados de Gestión de Incidentes; estas contrapartes se encuentran definidas en el registro "Contrapartes Gestiona.MINVU", ubicado en Trabajo Colaborativo/SSI/Subsecretaría.

5.1 Planificación y Preparación (A.16.01.01).

La eficaz gestión de incidentes de seguridad de la información requiere una planificación y preparación adecuada. Por lo anterior, el Ministerio de Vivienda y Urbanismo realiza las siguientes actividades preparatorias:

a) Elabora una Política Específica de Gestión de Incidentes de Seguridad de la Información, en la cual se establece el compromiso de la alta dirección con esa política;
b) Revisa anualmente las políticas de seguridad de la información y las actualiza cada vez que sea necesario;
c) Define y documenta el procedimiento de gestión de incidentes de seguridad de la información.
d) Establece un Equipo de Respuesta a Incidentes, con un programa de capacitación apropiado para el personal;
e) Establece y preserva relaciones y conexiones adecuadas con organizaciones internas y externas que están directamente involucradas en la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información;

g) Diseña y desarrolla un programa de conocimiento y capacitación para la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.

5.2 Detección y Reporte (A.16.01.02, A.16.01.03).

La detección y reporte de los eventos o debilidades de Seguridad de la Información en cada uno de los servicios puede ser realizada por todo el personal MINVU, así como también por asesores, consultores, practicantes, personas naturales o jurídicas que presten servicios para el MINVU. Adicionalmente, pueden ser reportados por el Computer Security Incident Response Team - **CSIRT**- (Equipo de Respuesta ante Incidentes de Seguridad de la Información) Nacional del Gobierno directamente al Encargado de Seguridad de la Información y Ciberseguridad de la Subsecretaría u otra autoridad de cada Servicio, según corresponda.

Es fundamental señalar que, al momento de la notificación del evento, quien reporta, debe entregar la mayor cantidad de información posible, incluyendo cualquier evidencia, en el formato en que esté disponible, que pudiera ser relevante para su estudio y análisis.

Se han definido tres categorías de eventos o debilidades, informático, no informático y sensible
A continuación, se establecen los tipos de eventos o debilidades y el encargado de recibirlos y registrarlos dependiendo de cada servicio:

5.2.1 Informáticos

Los eventos de tipo informático corresponden a sucesos que indica una posible brecha en la seguridad de la información o falla en el control de ésta asociados al ámbito tecnológico.

- **En el Nivel Central.**

Debe ser reportado al Analista MAU, a través del correo electrónico ayuda@minvu.cl o al anexo **1100**.

El Analista MAU registra el evento en el **Sistema Aranda**, evalúa si corresponde a un evento o debilidad de seguridad de la información y coordina las acciones para abordarlo.

- **SEREMI, SERVIU y PMS**

Debe ser reportado vía correo electrónico, llamada telefónica o personalmente al Coordinador Informático del Servicio, quien registra el evento en su Planilla de Eventos o sistema propio utilizado para tal fin; evalúa si corresponde a un evento o debilidad de seguridad de la información y coordina las acciones para abordarlo.
En caso que el evento supere la resolución de la región debe ser reportado a la mesa de ayuda en nivel central a través de correo electrónico (ayuda@minvu.cl) o del Sistema Aranda para su registro y tratamiento.

5.2.2 No informáticos

Los eventos de tipo no informático corresponden a sucesos que indican una posible brecha en la seguridad de la información o falla en el control de ésta asociados al ámbito de infraestructura, servicios generales, gestión de personas, seguridad física.

- **En el Nivel Central**

Debe ser reportado al Equipo DIVAD de acuerdo a la materia del evento según la siguiente tabla:

Materia	Responsable	Procedimiento
Gestión de Personas	Jefe Departamento de Gestión de Personas	Informar telefónicamente a los anexos **1560** o **1554** o personalmente a Jefe de Departamento Gestión de Personas o quien lo subrogue.
Infraestructura	Encargado Sección Infraestructura	Informar telefónicamente a los anexos **1395** o **1504** o a la Casilla infraestructura **infraestructura@minvu.cl**.
Servicios Generales / Oficina de Partes	Jefe Departamento de Compras y Servicios Generales	Informar telefónicamente a los anexos **1140**, **1135** o **1175** al Jefe Departamento de Compras y Servicios Generales.
Prevención de riesgos	Jefe Departamento de Prevención de Riesgos	Informar telefónicamente a los anexos **1370** o **1377**, de acuerdo Instructivo Procedimiento de Actuación frente a Accidentes del Trabajo.
Seguridad Física	Jefe de Seguridad	Informar telefónicamente al anexo **1196** o personalmente a Jefe de Seguridad o quien se encuentre en portería

Una vez recibido el reporte de un evento o debilidad, el Equipo DIVAD opera con sus propios procedimientos y protocolos para la atención inmediata del mismo. Sin perjuicio de lo descrito anteriormente, el Equipo DIVAD revisa a lo menos cada tres meses los eventos o debilidades reportados, identificando en el Acta de la reunión si corresponden o no a eventos de seguridad de la información.

- **En las SEREMI, SERVIU y PMS**

Debe ser reportado vía correo electrónico, llamada telefónica o personalmente al Coordinador del Área de Administración pertinente, o en quien delegue la función el Jefe de Servicio, quien registra en su Planilla de Eventos o Acta de Reunión o sistema propio utilizado para tal fin, evalúa y coordina acciones para abordar los eventos o debilidades de seguridad de la información no informáticos y genera la acción inmediata de acuerdo a sus propios procedimientos o protocolos.

En el caso que quien detecte el evento o debilidad sea un usuario o proveedor externo, deberá reportarlo a su contraparte técnica del MINVU vía correo electrónico, llamada telefónica o personalmente, quien a su vez deberá relevarlo de acuerdo a lo anteriormente expuesto.

5.2.3 Sensibles

La excepción de eventos o debilidades de seguridad de la información a los canales de registro anteriormente expuestos lo constituyen los eventos o debilidades de tipo sensible que son sucesos que por sus características, personas, instrumentos o recursos que involucra, deben ser informados de manera confidencial a la organización para su respuesta y solución, por ejemplo, sucesos que tengan relación con la probidad, honorabilidad o dignidad de una persona.

Estos sucesos se reportan a la Jefatura Inmediata a través de correo electrónico o personalmente, quien lo escala al Jefe de Servicio, este último decide el tratamiento y medidas a adoptar, definiendo además si éste es considerado un incidente de seguridad de la información y si el Encargado de Seguridad de la Información deberá registrarlo en el sistema Gestiona MINVU[2] de acuerdo al nivel de confidencialidad que requiera el evento en particular.

Si no fuese un evento o debilidad sensible, se solicita a quien lo reportó que siga el proceso de gestión de incidentes.

5.3 Evaluación y Decisión (A.16.01.04).

Una vez clasificado **un evento o debilidad** en categoría **"Seguridad de la Información"** se debe determinar **si corresponde a un incidente de seguridad de la información**.

Cabe destacar que un incidente de seguridad de la información corresponde a uno o varios eventos identificados que tienen una probabilidad significativa de comprometer las operaciones y amenazar la confidencialidad, integridad y/o disponibilidad de los activos de información.

Los Incidentes de seguridad de la información se clasifican en dos categorías:

- **Informáticos:** Todos aquellos incidentes que afecten las tecnologías de la información, mediante la violación de políticas, normas y procedimientos informáticos, o del ámbito de ciberseguridad. Por ejemplo:
  - Acceso lógico no autorizado: Todo tipo de ingreso y operación no autorizada a los sistemas, sea o no exitoso, tales como: robo de información, borrado de información, intentos recurrentes y no recurrentes de acceso no autorizado, abuso y/o mal uso de los controles de acceso de los servicios informáticos, entre otros.
  - Denegación de servicios computacionales.
  - Código malicioso: Introducción virus informáticos, troyanos, gusanos informáticos, etc.
  - Escaneos, pruebas o intentos de obtener información de redes o servidores sin autorización.
  - Mal uso de los recursos tecnológicos: Mal uso y/o abuso de servicios informáticos, violación de las normas de acceso a internet, mal uso y/o abuso del correo electrónico.

  Esta clasificación es responsabilidad del Analista MAU o el Coordinador Informático en caso de regiones, quienes en caso de dudas podrán comunicarse con el Encargado de Seguridad Informática del MINVU.

- **No Informáticos:** Todos aquellos incidentes no contemplados en el punto anterior, por ejemplo:
  - Robo de un documento.
  - Filtración de documentos con información clasificada.
  - Incidentes provocados por la naturaleza.
  - Acceso físico, no autorizado.
  - Pérdida de integridad de un proceso del servicio, entre otros.

  Esta clasificación es responsabilidad del Equipo DIVAD en Nivel Central y en regiones el Coordinador del Área de Administración o quien designe el jefe del servicio, quienes revisan a lo menos cada tres meses los eventos o debilidades reportados dejando evidencia de la revisión en el acta de la respectiva reunión, y si corresponde a un incidente de seguridad de la información procede a gestionarlo de acuerdo a lo descrito en el numeral 5.4 del presente procedimiento.

[2] **https://gestiona.minvu.cl/se**

Una vez que se ha determinado que el evento o la debilidad reportada corresponde a Incidente de Seguridad de la Información, el Encargado de Gestión de Incidentes procederá a realizar su registro en el sistema Gestiona MINVU. En la siguiente tabla se señala el Encargado de Gestión del Incidente dependiendo del tipo de incidente:

Tipo de Incidente	Seremi/Serviu/ PMS	Nivel Central
Informático	Coordinador Informático Encargado de Seguridad de la Información	Analista MAU Encargado de Seguridad Informática
No Informático	Coordinador del Área de Administración pertinente, o en quien delegue la función el Jefe de Servicio	Coordinador DIVAD

A continuación, el Encargado de Gestión del Incidentes, evalúa su impacto a través de los criterios definidos según la tabla siguiente, considerando la clasificación de IMPACTO para cada criterio:

IMPACTO	CLASIFICACIÓN		
⇨ Por **MAGNITUD** del Impacto *(Cantidad de activos afectados y alcance institucional)*	**ALTO** Afecta a toda la Seremi, Serviu o Nivel Central **3**	**MEDIO** Afecta a más de dos Áreas / Departamentos /Divisiones **2**	**BAJO** Afecta a un Área / Departamento/ División **1**
⇨ Por **DURACIÓN** estimada del evento.	**ALTO** Más de un día **3**	**MEDIO** Un día **2**	**BAJO** 4 Horas **1**
⇨ Por **CRITICIDAD** del activo afectado. *(Según el nivel de daño)*	**ALTO** Daño significativo de activo/s **3**	**MEDIO** Daño considerable de activo/s **2**	**BAJO** Daño menor de activo/s **1**

La evaluación de impacto de los criterios señalados, permite definir el orden de atención o tratamiento de los incidentes y el plazo máximo para su tratamiento; este es calculado automáticamente por el Sistema Gestiona MINVU arrojando una categorización de prioridad según el impacto calculado, pudiendo ser de carácter Urgente, Prioritario o Moderado, criterios que son parametrizados directamente en el sistema Gestiona MINVU.

Dependiendo del Nivel de Impacto con que se evalúe los incidentes de seguridad de la información, la oportunidad para su atención y tratamiento bajo acciones correctivas consideran los siguientes plazos predeterminados para su tratamiento:

Escala de Oportunidad en Solución de incidentes, según Nivel de Impacto	
Incidentes con prioridad URGENTE	Máximo 30 días para efectuar acciones
Incidentes con prioridad PRIORITARIO	Máximo 60 días para efectuar acciones
Incidentes con prioridad MODERADA	Máximo 6 meses para efectuar acciones

El tiempo máximo de tratamiento, puede ser ampliado de acuerdo a las características de la medida a tomar.

5.4 Contención y Respuesta (A.16.01.05).

Una vez determinado el impacto del incidente a través del sistema Gestiona.MINVU, el Encargado de Gestión de Incidentes debe realizar el análisis de causas, pudiendo utilizar técnicas como 5 porqués, lluvia de ideas, Ishikawa u otra metodología que considere pertinente, recopilando antecedentes que sean necesarios para determinar la o las causas que lo originaron.

El Encargado de Seguridad Informática (para Incidentes de Tipo Informáticos) o el Encargado de Seguridad de la Información, o en quien delegue esta función, (para Incidentes de Tipo No Informáticos), revisa que el Análisis de Causa corresponda al incidente registrado.

Una vez detectada la causa raíz y validada por el Encargado de Seguridad Informática o Seguridad de la Información, el Encargado de Gestión de Incidentes procede a generar el Plan de Acción a través del sistema Gestiona.MINVU, definiendo responsables y plazos de ejecución para abordar las causas encontradas y evitar que el incidente vuelva a ocurrir.

El Encargado de Seguridad Informática o Encargado de Seguridad de la Información, revisa que el Plan de Acción aborde las causas que originaron el incidente registrado.

Finalmente, una vez validado el Plan de acción, el responsable de las acciones debe ejecutarlas en el plazo definido, ingresar la evidencia de las acciones realizadas e informar su ejecución a través del sistema Gestiona MINVU.

En esta etapa se realiza seguimiento al tratamiento de los incidentes de seguridad de la información detectados y gestionados a través del sistema Gestiona MINVU, además de ejecutar acciones que contribuyan a la mejora continua de la gestión de incidentes.

Luego de máximo 3 meses después que las acciones comprometidas en el Plan de Acción se han informado como ejecutadas, el Encargado de Seguridad de la información del servicio define al responsable de determinar la eficacia, quien realiza la evaluación del plan de acción determinando si este fue eficaz o no y registrando el resultado de la evaluación en el Sistema Gestiona MINVU.

Si la gestión del incidente fue eficaz se cierra el plan de acción y el Encargado de Gestión de Incidentes coordina la respuesta a quien reportó el incidente de SI, dejando la evidencia en el mismo Sistema.

De no ser eficaz se debe presentar al Comité de Seguridad de la Información el cual evalúa acciones a tomar o escala el incidente al Jefe de Servicio quien define las acciones adicionales que considere pertinentes e informa al Encargado de Seguridad de la Información quien realizará las etapas de Gestión de Incidentes y Seguimiento a través del sistema Gestiona MINVU.

En caso que el incidente no esté bajo control y pueda comprometer la seguridad de la Institución o del País, el Encargado de Seguridad de la Información debe escalarlo al Computer Security Incident Response Team - CSIRT- (Equipo de Respuesta ante Incidentes de Seguridad de la Información) Nacional del Gobierno a través del correo electrónico csirt@interior.gob.cl.

5.5 Lecciones Aprendidas y Mejora (A.16.01.06).

Con el objetivo de garantizar el seguimiento del proceso de gestión de incidentes, el Comité de SSI revisará periódicamente el estado de los incidentes de seguridad de la información dando lugar a posibles cambios de plazos y ajustes que permitan corregir la causa raíz detectada.

El Encargado de Seguridad de la Información en Nivel Central, SERVIU y PMS, o en quien delegue esta función, al menos una vez al año recopila información sobre incidentes registrados, y elabora un **Informe de aprendizaje Gestión de Incidentes de Seguridad de la Información** considerando especialmente las causas analizadas y acciones efectuadas de los incidentes, con el propósito de generar análisis que permita, si corresponde, emprender mejoras en la Seguridad de la Información, reduciendo de este modo la probabilidad o impacto de incidentes futuros. Dicho informe será enviado al Comité Técnico de Nivel Central quien genera la información de la Subsecretaria además de consolidar y enviar a los/las Encargados/as de Seguridad de la Información del Sector, Jefes de Servicio y Comité de SSI de la Subsecretaría.

5.6 Recolección de Evidencia (A.16.01.07).

Cada Servicio resguarda y preserva las evidencias recopiladas a partir del tratamiento de incidentes de seguridad de la información a través del sistema Gestiona MINVU, siempre que sea posible, no vulnere derechos de terceros y, en general, no genere incumplimiento alguno al Estatuto Administrativo y demás normativa aplicable.

Una vez que un evento o debilidad es clasificado como un incidente de seguridad de la información, se deberá conformar un equipo de investigación, con la finalidad de recolectar la mayor cantidad de información que permita tener claridad absoluta respecto al incidente (informes técnicos internos y externos, entrevistas, impresiones de pantalla, etc.). Esta información quedará resguardada en el sistema Gestiona MINVU, siempre que sea posible y no vulnere derechos de terceros y, en general, no genere incumplimiento alguno al Estatuto Administrativo y demás normativa aplicable.

Toda aquella evidencia generada producto del proceso de investigación debe ser administrada exclusivamente por el equipo de investigación, bajo los criterios de confidencialidad, disponibilidad e integridad, y no ser compartida con otros funcionarios. El responsable de resguardar los registros será el Encargado de Seguridad de la Información.

6 INDICADORES

El indicador se calcula de forma semestral y se presenta ante el Comité de Seguridad de la Información cada vez que sea convocado, considerando los incidentes del periodo.

Nombre Indicador	Fórmula de Cálculo	Frecuencia
Porcentaje de incidentes tratados oportunamente según su nivel de impacto evaluado.	(N° de incidentes tratados en tiempos definidos* según el Impacto evaluado / N° Total de incidentes reportados de acuerdo al procedimiento de gestión de incidentes de seguridad de la información)*100	Semestral

Un incidente se considera tratado cuando su plan de acción se ha implementado, generando los medios de verificación correspondientes y dejando registro de ello en el sistema Gestiona MINVU.

*Los tiempos definidos se establecen en el punto 5.3 del presente procedimiento, tabla **"Escala de Oportunidad en Solución de incidentes, según Nivel de Impacto"**.

7 ANEXOS

Anexo 1: Diagrama de Flujo Procedimiento Gestión de Incidentes.

8 REFERENCIAS

- Política Específica de Gestión de Incidentes de SI
- Norma NCh-ISO 27001:2013

9 CONTROL DE REGISTROS

Los siguientes registros aplican para la Subsecretaría de Vivienda y Urbanismo (Nivel Central y 16 Seremi):

Nombre del Registro	Control	Almacenamiento	Protección	Recuperación	Retención	Disposición	Responsable
Difusión	A.16.01.01	Intranet-Trabajo Colaborativo	Clave según perfil usuario MINVU	Por año	Histórico	No Aplica	Encargado de Seguridad de la Información
Aranda	A.16.01.02	Sistema Aranda	Clave según perfil usuario MINVU	Por número	Histórico	No Aplica	Encargado de Seguridad Informática
Registro de Eventos SI Seremi	A.16.01.02 A.16.01.03	PC Coordinador Informático	Clave según perfil usuario MINVU	Por año	Histórico	No Aplica	Encargado de Seguridad de la Información
Acta DIVAD revisión eventos no informáticos	A.16.01.02 A.16.01.03 A.16.01.04	Intranet-Trabajo Colaborativo	Clave según perfil usuario MINVU	Por año	Histórico	No Aplica	Jefa DIVAD
Reporte de Incidentes	A.16.01.04 A.16.01.05	Sistema Gestiona MINVU	Clave según perfil usuario MINVU	Por número	Histórico	No Aplica	Encargado de Seguridad de la Información
Acta Comité SSI	A.16.01.06	Intranet-Trabajo Colaborativo	Clave según perfil usuario MINVU	Por fecha	Histórico	No Aplica	Encargado de Seguridad de la Información
Informe de Aprendizaje Gestión de Incidentes	A.16.01.06	Intranet-Trabajo Colaborativo	Clave según perfil usuario MINVU	Por año	Histórico	No Aplica	Encargado de Seguridad de la Información
Pantallazo Sistema Gestiona MINVU, o Informe de Evidencia	A.16.01.07	Sistema Gestiona MINVU	Clave según perfil usuario MINVU	Por número	Histórico	No Aplica	Encargado de Seguridad de la Información

Los siguientes registros aplican para los SERVIU y Parque Metropolitano de Santiago:

Nombre del Registro	Control	Almacenamiento	Protección	Recuperación	Retención	Disposición	Responsable
Difusión	A.16.01.01	Intranet-Trabajo Colaborativo	Clave según perfil usuario MINVU	Por año	Histórico	No Aplica	Encargado de Seguridad de la Información SERVIU y PMS
Reporte de Incidentes	A.16.01.04 A.16.01.05	Sistema Gestiona MINVU	Clave según perfil usuario MINVU	Por número	Histórico	No Aplica	Encargado de Seguridad de la Información SERVIU y PMS
Registro Eventos SI Seremi/Serviu	A.16.01.02 A.16.01.03	PC Coordinador Informático	Clave según perfil usuario MINVU	Por año	Histórico	No Aplica	Coordinador Informático SERVIU y PMS
Informe de Aprendizaje Gestión de Incidentes	A.16.01.06	Intranet-Trabajo Colaborativo	Clave según perfil usuario MINVU	Por año	Histórico	No Aplica	Encargado de Seguridad de la Información SERVIU y PMS
Pantallazo Sistema Gestiona MINVU, o Informe de Evidencia	A.16.01.07	Sistema Gestiona MINVU	Clave según perfil usuario MINVU	Por número	Histórico	No Aplica	Encargado de Seguridad de la Información

10 REGISTROS DE OPERACIÓN

Semestralmente, la segunda quincena del mes de agosto y del mes de diciembre, el Coordinador Nacional SSI y Ciberseguridad o el Encargado de Seguridad de la Información en regiones, elabora un Informe de Gestión de Incidentes que contiene el resultado de la operación de los controles comprometidos por su Servicio.

Nombre del Registro	Control	Frecuencia/ Periodicidad	Responsable
Informe de Gestión de Incidentes	A.16.01.01-A.16.01.07	Semestral	Coordinador Nacional SSI y Ciberseguridad / Encargado de Seguridad de la Información

A partir del año 2020 se realizará en forma semestral, sin embargo, el año 2019 se realizará mensualmente.

11 CONTROL DE CAMBIOS (Últimas tres modificaciones)

Versión	Fecha	Principales puntos modificados
04	23.12.2016	- Se reformula por completo y se establece a nivel ministerial.
05	28.07.2017	- Revisión puntos de contacto y reestructuración del procedimiento - Se incorporó el rol del CSIRT de Gobierno - Se incluyó el Informe de Aprendizaje de Gestión de Incidentes - Se agregó el punto 9 NOMENCLATURA
06	13.09.2019	Se reestructura el procedimiento, no teniendo cambios los registros de operación.

Actualizado por:	Revisado por:	Aprobado por:
Marcela Jara Cartes	Andrea Ubal Espinoza/ Claudia Hidalgo Pérez Encargados/as y coordinadores SSI de SEREMI/ SERVIU/PMS	Marcela Acuña Gómez
Cargo/Dependencia: Analista Departamento de Planificación y Control de Gestión	**Cargo/Dependencia:** Jefe Sección Control de Gestión/ Asesora Subsecretaría Encargados/as y coordinadores SSI de SEREMI/ SERVIU/PMS	**Cargo/Dependencia:** Encargada de Seguridad de la Información

II. **Establécese** la obligación del Encargado/a de Seguridad de la Información de la Subsecretaría de Vivienda y Urbanismo de difundir el procedimiento fijado por este instrumento 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. Se deja constancia que la presente Resolución no irroga gastos para el presupuesto de este Ministerio.

ANÓTESE, NOTIFÍQUESE, 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/ACA/AUE

DISTRIBUCIÓN:
- Gabinete Ministro V. y U.
- Gabinete Subsecretario V. y U.
- SEREMI (16)
- 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