Ministerio de Vivienda y Urbanismo

Gobierno de Chile

APRUEBA POLÍTICA ESPECÍFICA DE PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE 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 2953

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, (SEGPRES), de 2004; 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; el Instructivo Presidencial Nº 08/2018, que Imparte Instrucciones Urgentes en Materia 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, en materia de seguridad de la información, se han dictado una serie de normas entre las que destacan el D. S. Nº 83, (SEGPRES), de 2004, que aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos y 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.

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 ello, 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. **Apruébase** la Política Específica de Planificación de la Continuidad de la Seguridad de Información, versión 01, para ser implementada en los 16 Servicios de Vivienda y Urbanización, en el Parque Metropolitano de Santiago y en la Subsecretaría de Vivienda y Urbanismo (Nivel Central y sus 16 Secretarías Regionales Ministeriales de Vivienda y Urbanismo), la que se detalla a continuación:

MINISTERIO DE VIVIENDA Y URBANISMO - DIVISIÓN JURÍDICA

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

"POLÍTICA ESPECÍFICA DE PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE INFORMACIÓN"

1. OBJETIVO

Esta política establece directrices para planificar la continuidad de la seguridad de la información ante situaciones adversas que puedan provocar interrupciones en la gestión de seguridad de la información asociada a los procesos críticos de la Institución.

2. ALCANCE

La presente Política, considerada como parte del Dominio de Aspectos de Seguridad de la Información en la gestión de continuidad del negocio, en particular del control A.17.01.01 Continuidad de la Seguridad de la Información de la norma NCh-ISO 27001:2013, es aplicable ante la ocurrencia de situaciones adversas, ya sea, durante una crisis o desastre en las dependencias de los 16 Servicios de Vivienda y Urbanización, en el Parque Metropolitano de Santiago, y en la Subsecretaría de Vivienda y Urbanismo (Nivel Central y sus 16 Secretarías Regionales Ministeriales de Vivienda y Urbanismo), para los procesos críticos de los definidos en el alcance del Sistema de Seguridad de la Información.

Esta política debe ser cumplida por todos los usuarios del Ministerio, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo las empresas que presten servicios al MINVU.

3. NOMENCLATURA

GCN: Gestión de Continuidad del Negocio.

MTPD Maximum tolerable period of disruption- Tiempo Máximo Tolerable de Interrupción: Es aquel plazo después del cual la viabilidad del MINVU se verá amenazada de forma irrevocable (financiera, pérdida de reputación, etc.) de no poder reiniciar la entrega de un producto, proceso o servicio específico. Debe ser definido por el propietario de la entrega del producto, proceso o servicio y aprobado por la Dirección.

RPO Recovery Point Objective:

Desde la perspectiva del responsable del servicio: es el tiempo transcurrido desde la última copia de respaldo antes de ocurrida una crisis o desastre.

Desde la perspectiva del usuario: es la tolerancia máxima de pérdida de datos de cada aplicación o servicio de tecnología de información.

RTO Recovery Time Objective- Tiempo Objetivo de Recuperación: es uno de los resultados clave del BIA que identifica el tiempo requerido para llevar a cabo las actividades claves para la recuperación de las operaciones y/o sus dependencias

BIA: Business Impact Analysis: es un análisis a nivel ejecutivo por medio del cual una organización determina de manera cuantitativa y cualitativa impactos, efectos y pérdidas que podrían suceder-de sufrir la organización un evento mayor, crisis o desastre. Establece las funciones y procesos críticos, sus prioridades de recuperación e interdependencia a fin de determinar tiempos de recuperación objetivo (RTO) y puntos objetivo de recuperación (RPO). Los resultados del BIA son utilizados para la toma de decisiones respecto a las estrategias de recuperación.

4. DOCUMENTOS RELACIONADOS.

- Política General de Seguridad de la Información.
- Norma Chilena ISO 27001:2013.

5. ROLES Y RESPONSABILIDADES.

Jefe/a Superior de Servicio

- Responsable de fijar los recursos necesarios para garantizar la continuidad de la Seguridad de la Información y de comunicar a las autoridades del Ministerio la activación de los planes de continuidad de la seguridad de la información.

Jefe DINFO

- Encargado de asegurar la entrega y provisión de equipamiento y tecnologías que soporten los procesos críticos de acuerdo a los requisitos de seguridad y continuidad de la seguridad de la información ante eventos de interrupción.

Encargado de Seguridad Informática

- Determinar los requisitos de seguridad y continuidad de la seguridad de la información para la gestión de la seguridad informática.
- Determinar los recursos mínimos necesarios para la recuperación de la gestión de la seguridad de la información.

Encargado/a de Seguridad de la Información

- Revisar y verificar que los requisitos de seguridad y continuidad de la seguridad determinados cubran en forma razonable la seguridad necesaria de los procesos críticos y su ~~la~~ continuidad ante los eventos de interrupción.
- Responsable de asegurar la continuidad de la seguridad de la información sea permanente y conducida metodológicamente.
- Velar por el cumplimiento de la presente Política.

Encargado de Continuidad del Negocio

- Responsable de asegurar que la GCN sea permanente y conducida metodológicamente.

6. REGLAS DE LA POLÍTICA

La razón de ser de la Gestión de la Seguridad de la Información es posibilitar la operación normal de los procesos de la Institución en un entorno seguro. Ante la eventual posibilidad que un riesgo de seguridad de la información cause la interrupción de las operaciones o la no disponibilidad de los recursos que las soportan (instalaciones, personas, terceros, equipamiento y tecnologías), se deben establecer los requisitos de seguridad y de continuidad de la seguridad para los procesos críticos.

Los **requisitos de seguridad** se refieren a las necesidades de gestión de seguridad y los recursos que la soportan para que los procesos críticos puedan operar en un entorno seguro, mientras que los **requisitos de continuidad** se refieren a las necesidades de recuperación de esta gestión de seguridad y los recursos que la soportan ante un evento de interrupción de los procesos críticos.

La gestión de la continuidad de la seguridad de la información deberá considerar 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, de corresponder; los componentes informáticos y no informáticos de apoyo y las acciones de recuperación ante contingencias menores y mayores.

La continuidad de la seguridad de la información se incluye en el Procedimiento de Gestión de Continuidad de la Seguridad de la Información del Servicio.

6.1 Planificación

6.1.1 Continuidad y requisitos de seguridad

Se deben identificar los requisitos de seguridad y continuidad de la seguridad de información para responder al nivel necesario de continuidad para la gestión de seguridad ante situaciones adversas y garantizar que los procesos críticos se recuperen considerando los aspectos de seguridad.

El Encargado de Seguridad de la Información deberá revisar y verificar que los requisitos de seguridad y continuidad de la seguridad determinados en la presente política y en el Análisis de Impacto al Negocio (BIA), cubran en forma razonable la seguridad necesaria de los procesos críticos y la continuidad ante los eventos de interrupción.

El Jefe de la División Informática deberá asegurar la entrega y provisión de equipamiento y tecnologías que den soporte a los procesos críticos de acuerdo a los requisitos de seguridad y continuidad de la seguridad de la información ante eventos que supongan su interrupción.

En el caso de la gestión de continuidad de la seguridad de la información se aplican los siguientes principios que la sustentan:

- La continuidad de la seguridad de la información se integra con la continuidad del negocio.
- Los requisitos de seguridad de la información para garantizar niveles adecuados de confidencialidad, integridad y disponibilidad ante situaciones adversas que afecten la continuidad son:
    - Gestión de Antivirus.
    - Gestión de Monitoreo y seguridad Perimetral.
    - Gestión de Incidentes.
    - Gestión de Riesgos de seguridad de la información.
    - Gestión de Controles de seguridad.
    - Gestión de Actualizaciones de seguridad.

- Cada uno de los procesos críticos de seguridad de la información tanto internos como externos se identifica y enumeran, en orden de criticidad, en concordancia con el Plan de Continuidad del MINVU.

- Los activos de información crítica que están involucrados en cada proceso se identifican y hacen referencias cruzadas a los registros de activos.

- Para cada uno de los procesos críticos definidos en el alcance del SSI, se identifican los riesgos de desastres, fallas de seguridad o equipos, pérdida de servicio, ataques y pérdida de disponibilidad de servicio) que puedan afectar la continuidad de las actividades del MINVU.

- Para cada uno de los riesgos se definen los posibles impactos en la continuidad de la seguridad de la información que se generarían en el MINVU, que van desde la pérdida de las claves de entrada al sitio hasta la pérdida de los sitios.

- Los riesgos se priorizan en términos de sus impactos en las actividades y funciones realizadas en el MINVU y el proceso de planificación de la continuidad de la seguridad de la información supone el tomar acuerdos para hacer frente a estos riesgos en relación a la prioridad antes mencionada.

- El Plan de continuidad de la seguridad de la información aborda todos los componentes de continuidad de la información de las actividades del MINVU y garantiza que se disponga de

recursos capacitados adecuados para dar continuidad a todos los activos de seguridad de la información identificados, incluida la adopción de las medidas adecuadas para la protección de los empleados, la información procesada por ellos y las localidades donde estos ejecutarán el trabajo.

6.1.2 Análisis de impacto al negocio

Se deben identificar las necesidades de recuperación de la gestión de la seguridad de la información y los recursos que les sirve de soporte (instalaciones, personas, terceros, equipamiento y tecnologías), para lo cual:

Los Jefes de Unidades Orgánicas deben:

- Identificar los procesos críticos, sus entradas / salidas y sus dependencias de otros procesos. Asimismo, se debe determinar las necesidades de seguridad de la información que aseguran los procesos críticos.
- Determinar el impacto en el cumplimiento, operación e imagen de la Institución, que provocaría la interrupción de cada proceso crítico y el MTPD.
- Determinar, en conjunto con el Encargado de Seguridad de la Información y el Encargado de Seguridad Informática, los requisitos de seguridad y continuidad de seguridad de la información para los procesos críticos y la gestión de la seguridad de la información.
- Determinar, en conjunto con el Encargado de Seguridad de la Información y el Encargado de Seguridad Informática, los recursos mínimos necesarios para la recuperación de los procesos críticos y la gestión de la seguridad de la información tales como instalaciones, personas, terceros, equipamiento y tecnologías, así como sus necesidades de recuperación (RPO y RTO según aplique).

7. DIFUSIÓN

La comunicación y difusión de la presente Política específica es responsabilidad del Encargado/a de Seguridad de la Información o en quien se designe esta función, pudiendo utilizar para ello los canales de difusión establecidos, como publicación en la Intranet institucional y/o Minvuletín, Correo electrónico, Afiches, 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 ante requerimiento de algún Servicio, 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, 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; Viviana Peña Morales/ Analista Depto. Planificación y Control de Gestión, División Finanzas, Marcela Jara Cartes/ Analista Depto. Planificación y Control de Gestión, División Finanzas.

Revisado por:

Marcela Acuña Gómez, Encargada de Seguridad de la Información; 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 el presente instrumento por el Encargado/a de Seguridad de la Información de cada Servicio 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 cada Servicio las acciones tendientes a su implementación en materias de su competencia.

IV. La presente resolución no irroga gastos para el presupuesto del 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

CMMV/MAG/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