Ministerio de Vivienda y Urbanismo

Gobierno de Chile

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

DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 14.484, (V. Y U.), DE 2017, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE RESPALDO Y RETENCIÓN DE LA INFORMACIÓN, EN EL MARCO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO.

SANTIAGO, 30 DIC 2019

RESOLUCIÓN EXENTA N° ___3076

HOY SE RESOLVIO LO QUE SIGUE

VISTOS:

Lo dispuesto en el D.L N° 1305, 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 el Instructivo Presidencial N° 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 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, en materia de seguridad de la información, se han dictado una serie de normas 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, y la 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 N°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.

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.

d. La necesidad de actualizar la Política Específica de Seguridad de Respaldo y Retención de la Información aprobada por Resolución Exenta 14.484, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

I. **Derógase** la Política Específica de Seguridad de Respaldo y Retención de la Información aprobada por Resolución Exenta 14.484, (V. y U.), de 2017.

II. **Apruébese** la Política Específica de Seguridad de Respaldo y Retención de la Información, la que se detalla a continuación:

"POLÍTICA ESPECÍFICA DE SEGURIDAD DE RESPALDO Y RETENCIÓN DE LA INFORMACIÓN".

1. OBJETIVO

Esta política establece las reglas para gestionar los respaldos de información requerida por el MINVU.

2. ALCANCE

La presente Política, considerada como parte del Dominio de Seguridad de las Operaciones, se aplica al respaldo, retención y protección de toda información contenida en los servidores centrales, estaciones de trabajo y equipos de comunicaciones.
Esta política debe ser cumplida por todos los usuarios del Ministerio 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 un acto administrativo mediante el que se manifiesta tal voluntad.

Esta política está relacionada con el cumplimiento del control A.12.03.01 de la norma NCh ISO 27001:2013, para todos los procesos/productos estratégicos dentro del alcance del SSI.

3. DOCUMENTOS RELACIONADOS.

- Normativa de gestión de infraestructura de TI

4. ROLES Y RESPONSABILIDADES.

Encargado/a de Seguridad de la Información y Ciberseguridad

- Velar por el cumplimiento y revisión de las Políticas basada en requisitos de negocio y seguridad de la información.

Dueño de los datos

- Solicitar y/o autorizar los respaldos o la restauración de los datos a su cargo cuando corresponda

Jefatura de sección ingeniería y explotación de sistemas

- Establecer y aplicar los procedimientos de respaldos y restauración
- Gestionar las tareas asociadas a los respaldos y restauración de la información

Jefatura departamento de soporte tecnológico a la gestión

- Gestionar tareas de respaldos y restauración para estaciones de trabajo

Coordinador informático regional

- Aplicar los procedimientos de respaldos y restauración asociados a su región

Jefaturas de división de informática

- Solicitar respaldos para los sistemas de información requeridos

Usuarios de estaciones de trabajo

- Hacer la copia de la información indispensable para la gestión operativa del servicio

5. REGLAS DE LA POLÍTICA

5.1 Protección de los respaldos de información.

- La información de los sistemas de información será protegida mediante respaldos.
- Se mantendrá un registro de los respaldos y una descripción en los medios magnéticos.
- Se mantendrá un registro del traslado de los medios magnéticos.
- La información será respaldada en medios magnéticos reservados para dicha tarea.
- La información contenida en los respaldos será almacenada de forma cifrada.
- Los respaldos se mantendrán en un ambiente protegido contra acceso no autorizado.
- Se mantendrán copias de respaldos ubicados fuera de la institución.
- Los medios magnéticos en tránsito serán protegidos contra acceso no autorizado y cualquier daño físico que surja durante el traslado y el almacenamiento.
- Si el medio magnético de respaldo se encuentra próximo a su vencimiento, la información contenida en él deberá ser traspasada a otro medio de respaldo de características similares.
- Ante un cambio tecnológico que se produzca en los medios de respaldo, que pueda generar obsolescencia tecnológica, deben generarse las acciones necesarias de resguardo de la información contenida en ellos.

5.2 Frecuencia, retención y vigencia de los respaldos

- La retención del respaldo de la información estará basada en los decretos, normativas y legislación vigente o por el plazo que la Institución haya definido.
- Se establecerán frecuencias y tipos de respaldo según la criticidad de la información. Todos los datos financieros, contables, legales y tributarios deben ser retenidos o de acuerdo con la normativa o reglamentación vigente.

5.3 Pruebas de restauración

- Se deben realizar pruebas periódicas de restauración de la información respaldada.
- Las pruebas de restauración serán acordes al plan de continuidad del negocio.
- Ante la detección de respaldos fallidos se aplicarán las medidas correctivas necesarias.

5.4 Borrado, respaldo y restauración de información en computadores personales del MINVU.

- El usuario sólo debe almacenar en las estaciones de trabajo información de apoyo personal para realizar sus funciones.
- Cuando los usuarios dada sus funciones requieran compartir información de apoyo asociada a procesos de negocio deberán informar a la mesa de atención de usuarios o al coordinador informático de la región.
- Si el usuario detecta que su computador de escritorio contiene información crítica asociada a un proceso de negocio deberá informar a la mesa de atención de usuarios o al coordinador informático de la región.
- Se dispondrán medios de almacenamiento para compartir información de apoyo al negocio, sujeto a previa evaluación de riesgo ante perdidas de información.
- Los medios de almacenamiento para compartir información de apoyo al negocio serán limitados, su disposición estará sujeta a disponibilidad de recursos y a evaluación de riesgo ante perdidas de información.
- Los medios de almacenamiento dispuestos serán respaldados ante perdidas de información.
- Es responsabilidad del usuario el resguardo de su información de apoyo en los medios de almacenamiento dispuestos según corresponda.
- Ante el cambio de un computador personal el técnico especialista y encargado de dicha función deberán respaldar la información de apoyo personal que indique el usuario para lo cual se dispondrá de un espacio de almacenamiento temporal para ello.
- Finalizado el cambio del computador personal la información deberá ser eliminada del medio de almacenamiento temporal previa conformidad y aceptación del usuario.
- Ante la reasignación o la baja de un computador personal la información deberá ser previamente borrada por el usuario en conjunto con el personal técnico especialista.

5.5 **Borrado de la información.**

- Finalizado el periodo de retención se borrará toda la información contenida en los medios magnéticos.
- Los medios magnéticos serán destruidos antes de darlos de baja.
- La información contenida en los medios de almacenamiento que no sea necesaria debe ser borrada de forma segura, de modo de evitar su recuperación
- Debe existir un registro preciso y completo de los activos eliminados o destruidos.

6. DIFUSIÓN

La comunicación y difusión de la presente política específica es responsabilidad de cada Encargado/a de Seguridad de la Información o en quien se designe para esta función, pudiendo usar para ello los canales de difusión establecidos, como Intranet, correo electrónico y Minvuletín, entre otros.
Adicionalmente, las Políticas específicas se encuentran publicadas en la página web del MINVU en el banner MINVU/Sobre MINVU.

7. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

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

8. CONTROL DE VERSIONES

N° Versión	Fecha Aprobación	Motivo de la revisión
01	Diciembre 2012	Versión inicial
02	Diciembre 2015	Actualización de la política.
03	Noviembre 2017	Se actualizan "Considerando" y "Objetivo"
04	Noviembre 2019	Se actualiza resolución de la nueva política general de seguridad de la información y pie de firma de autoridades

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;

Revisado por:
Marcela Acuña Gómez, Encargada de Seguridad de la Información; Agustín Goñi Gonzalez / jefe División de Informática.

III. **Establécese** la obligación del Encargado/a de Seguridad de la Información de la Subsecretaría de difundir la política fijada por este instrumento y en coordinación con el Comité de Seguridad de la Información velar por su estricto cumplimiento.

IV. **Realícense** por el jefe de la División de Informática las acciones tendientes a su implementación en materias de su competencia.

V. 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

MIMV/MAG/AGG/CPP/LCC

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

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

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
- Programa Aldeas y Campamentos
- Sistema Integrado de Atención a la Ciudadanía (SIAC)
- Depto. Comunicaciones
- Centro de Estudios Ciudad y Territorio Depto.
- Planificación y Control de Gestión DIFIN
- Oficina de Partes