

DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 14.495, (V. Y U.), DE 2017, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE CONTROL DE ACCESO FÍSICO, 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° 3071

VISTOS:

HOY SE RESOLVIO LO QUE SIGUE

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 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 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, 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.
- d. La necesidad de actualizar la Política Específica de Control de Acceso Físico aprobada por Resolución Exenta 14.495, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

- I. **Derógase** la Política Específica de Seguridad de Control de Acceso Físico, aprobada por Resolución Exenta 14.495, (V. y U.), de 2017.
- II. **Apruébase** la Política Específica de Seguridad de la Información relativa al Control de Acceso Físico, la que se detalla a continuación:

"POLÍTICA ESPECÍFICA DE SEGURIDAD DE CONTROL DE ACCESO FÍSICO"

1. OBJETIVO

Esta política define las reglas para el control de acceso físico de personas y equipos, a las áreas críticas que el MINVU define.

2. ALCANCE

La presente Política, considerada como parte del Dominio de control de acceso, se aplica a todas las áreas y en particular las áreas definidas como críticas, como el centro de cómputos ubicado en el edificio de la Subsecretaría nivel central. Es aplicable a 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 manifieste tal voluntad.

Esta política está relacionada con el cumplimiento del control A.09.01.01 de la norma NCh ISO 27001:2013, para todos los procesos/productos estratégicos dentro del alcance del SSI.

3. DOCUMENTOS RELACIONADOS.

- Resolución Exenta N° 1445 del 25.06.2019 Aprueba Procedimiento de Control de Acceso a la Sala de Servidores del MINVU.
- ORD N°0100 del 21.01.2019, reitera instrucciones para el uso de credencial institucional.
- Resolución Exenta N° 9668 del 30.12.2013 - Manual de Procedimientos de la administración y disposición de los bienes fiscales del MINVU.

4. ROLES Y RESPONSABILIDADES.

División Administrativa/ En regiones, quien designe el Seremi para dicha tarea / Departamentos o Áreas de Administración SERVIU/PMS

- Disponer los mecanismos de control físico para el acceso a áreas críticas.
- Mantener un inventario actualizado de los equipos computacionales.

División Informática, Subsecretaría de Vivienda y Urbanismo

- Llevar registro de todas las personas que acceden al data center.
- Solicitar autorización para el acceso al data center.

Jefes de Servicio y Jefaturas de División (o quien designe para ello).

- Definir áreas críticas de su dependencia.
- Autorizar el acceso a áreas críticas de su dependencia.

Encargado/a de Seguridad de la Información y ciberseguridad

- Velar por el cumplimiento de esta política.

5. REGLAS DE LA POLÍTICA.

5.1. Acceso a las dependencias, según perímetros de seguridad

- Para el edificio de la Subsecretaría Nivel Central, se resguarda el perímetro de seguridad a través de rejas en el acceso, controlado por guardias, cámaras de seguridad, comunicación radial entre guardias de edificio y el uso de tarjetas magnéticas para el ingreso a las oficinas. Las regulaciones para el Uso de credencial y control de acceso se encuentran establecidas en el ORD 0321, de 2013, sobre instrucciones para el uso de credencial y control de acceso.
- Asimismo, cada Servicio identifica y establece los perímetros de seguridad física con los que cuenta en su infraestructura a partir de uno o más documentos vigentes asociados a la seguridad física, considerando especialmente las dependencias en donde cada Institución ha evaluado pertinente contar con medidas de seguridad para los accesos físicos.

5.2. Áreas críticas en la Organización

- Las áreas críticas de la Subsecretaría se desprenden del inventario de activos (Ubicación), y corresponden a aquellas áreas donde se encuentren ubicados los activos definidos como críticos.
- Cualquier área que sea definida como crítica, deberá ser protegida bajo estas regulaciones, contar con un acceso restringido y controlado, que permita asegurar que solo ingresa el personal (o terceros) debidamente autorizado.
- El ingreso de los funcionarios autorizados en forma permanente a áreas críticas requiere de una declaración formal en que se identifique claramente la identidad del personal autorizado, con el fin de controlar el ingreso y revisar dicha nomina en forma periódica.
- El acceso por personal no habitual o personas externas debe ser autorizado por la Jefatura respectiva o por quien este faculte para ello, sin lo cual no se dará acceso al personal y/o personas externas.
- La Institución ha definido inicialmente que las áreas que contienen los equipos centrales de procesamiento (Data center Nivel Central), son críticas para el desarrollo normal de los procesos, por lo cual deben ser protegidos de accesos no autorizados a través de un procedimiento de control de acceso a la sala de servidores del MINVU.
- El responsable de cada dependencia de la Subsecretaría define las instrucciones generales para el acceso a las áreas críticas (si aplica).
- En el caso de las SEREMI es el Secretario Regional Ministerial, o quien designe para dicha tarea, el responsable de generar y difundir instrucciones al respecto.
- Por último, en el caso de SERVIU/PMS, es el/la director/a de Servicio, o quien éste/a designe, quien establece las instrucciones generales para el acceso a las áreas críticas (si aplica) para cada una de sus dependencias, correspondiendo la responsabilidad de generar y difundir tales instrucciones al Departamento o Área de Administración.

5.3. Acceso a equipos computacionales y dispositivos en áreas críticas

- Todo ingreso o egreso de equipos de computación o de comunicaciones en el centro de datos de la Subsecretaría, debe ser autorizado y coordinado por la Sección de Ingeniería y Explotación de sistemas dependiente de la División de Informática de la Subsecretaría.
- En la Subsecretaría, los traslados de equipos deben ser adecuadamente registrados, de acuerdo a los procedimientos establecidos en Resolución Exenta N° 9668 del 30.12.2013 – Manual de Procedimientos de la administración y disposición de los bienes fiscales del MINVU.
- A todo equipo de computación o de comunicaciones que no esté debidamente rotulado como propiedad de la institución, se le deben aplicar controles de seguridad de acceso a la red.

- Los equipos ingresados a estas áreas, en forma temporal por terceros, deben ser anotados en libro de bitácora de acceso al área crítica para su adecuado control de entrada y salida, no permitiendo su ingreso sin la debida rotulación o identificación.
- En el caso de SERVIU/PMS, los traslados de equipos igualmente deben ser registrados y ceñirse a procedimientos preestablecidos que resguarden su disponibilidad e integridad, debiendo establecerse un responsable para tal efecto.

5.4. Revocación de Accesos.

- Con ocasión del cambio de cargo de un funcionario, sus Jefaturas directas deben revisar sus permisos de acceso físico asignados y verificar que éstos sigan siendo válidos de acuerdo a su nueva función.
- En caso del término de la relación laboral de un funcionario con el MINVU, es responsabilidad de las Jefaturas directas informar formalmente esta situación, en el caso de la Subsecretaría, a la División Informática de estas situaciones, para proceder a revocar los accesos de acuerdo a lo establecido en el Procedimiento de Egreso de Personas.
- En el caso de SERVIU/PMS, cada Jefatura Directa debe informar y gestionar la remoción de accesos según el procedimiento para el egreso de personas que tengan debidamente establecido.

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.

Así mismo, 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

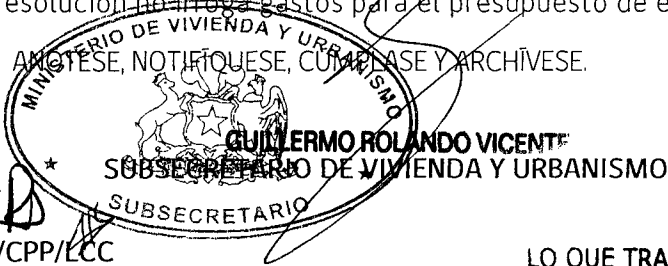
Nº Versión	Fecha Aprobación	Motivo de la revisión
01	Diciembre 2012	Versión inicial
02	Diciembre 2013	Incorporación de definiciones institucionales
03	Noviembre 2017	Se actualizan "Considerando" y "Objetivo"
04	Noviembre 2019	Se actualiza resolución de la nueva política general de seguridad de la información y pie de firma de autoridades

Elaborado por:
Leonardo Cavieres Córdoba/ Encargado de Seguridad Informática, División de Informática; Claudio Paredes Pizarro/ Jefe 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; Claudia Ernst Valencia/ Jefe División Administrativa.

- 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.

ANOTESE, NOTIFIQUESE, CUMPLASE Y ARCHÍVESE.



MIMV/MAG/AGG/CPP/LCC

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

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO


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

