



DEJA SIN EFECTO RESOLUCIÓN EXENTA Nº 14.487, (V. Y U.), DE 2017, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE ESCRITORIOS Y PANTALLAS LIMPIAS, EN EL MARCO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE VIVIENDA Y URBANISMO.

30 DIC 2019
SANTIAGO,

RESOLUCIÓN EXENTA Nº 3077/

VISTOS:

HOY SE RESOLVIÓ LO QUE SIGUE

Lo dispuesto en el D.L Nº1305, 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, en materia de seguridad de la información, se han dictado una serie de normas entre las que se encuentra el Decreto Supremo Nº 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 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.
- d. La necesidad de actualizar la Política Específica de Seguridad de Pantallas y Escritorios Limpios aprobada por Resolución Exenta 14.487, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

- I. **Derógase** la Política Específica de Seguridad de Pantallas y Escritorios Limpios aprobada por Resolución Exenta 14.487, (V. y U.), de 2017.
- II. **Apruébese** la Política Específica de Seguridad de escritorios y pantallas limpias, la que se detalla a continuación:

“POLÍTICA ESPECÍFICA DE SEGURIDAD DE ESCRITORIOS Y PANTALLAS LIMPIAS”

1. OBJETIVO

Esta política establece las reglas para proteger el equipamiento de daños producto de descuidos o accidentes, así como también proteger la información de la institución de accesos no autorizados a ella.

2. ALCANCE

La presente política es considerada como parte del dominio de seguridad física y del ambiente y aplica 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, a quienes se les otorgue una casilla de correo electrónico.

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.11.02.08 y A.11.02.09 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 Control de Acceso

4. ROLES Y RESPONSABILIDADES

Encargado/a de Seguridad de la Información y Ciberseguridad

–Velar por el cumplimiento de esta política.

Jefe División de Informática

–Definir e implementar las políticas de protección automatizadas que apoyen esta política.

Jefaturas Directas

–Velar por el cumplimiento de esta política.

Usuarios

–Cumplir con las definiciones establecidas en esta política.

5. REGLAS DE LA POLÍTICA

5.1. Equipos de usuarios no supervisados

–Para los escritorios de los funcionarios del MINVU que se encuentren en, o cercanos a una zona de atención o tránsito de público, las jefaturas directas deben implementar los mecanismos de seguridad de forma que la pantalla de la estación de trabajo no pueda ser vista por terceras personas.

– Se debe concientizar y advertir a todos los usuarios del MINVU de los requisitos y procedimientos de seguridad para proteger los sistemas y equipamiento asignado, cuando deje de usarlo por tiempo prolongado o al terminar las actividades, así como de su responsabilidad de no implementar tal protección.

–Se debe proteger con un mecanismo de bloqueo automático de pantalla y/o teclado controlado por contraseña, las aplicaciones, sistemas o equipo asignado por el MINVU, cuando deje de usarlo por tiempo prolongado o al terminar las actividades.

- Los dispositivos de almacenamiento removibles (pendrive, cd, discos, DVD, etc.), deben ser protegidos mediante el uso de algoritmos de cifrado de información y mediante seguridad física, como cajas con sellos (llaves).

5.2. Protección en escritorios y estaciones de trabajo del MINVU.

- Ante una ausencia prolongada de su lugar de trabajo, todo funcionario debe asegurarse que la información que utiliza debe quedar fuera del alcance de terceros.
- En el caso de información en papel se debe procurar que la información no sea vista por terceras personas.
- No escribir contraseñas ni otros datos sensibles en papeles o documentos que queden a la vista de terceras personas no autorizadas.
- No está permitido que el usuario intervenga físicamente el equipo computacional. Esta función está limitada a personal técnico calificado y autorizado.

5.3. Impresoras limpias

- Cualquier información que va a ser impresa en cualquier impresora, debe ser retirada de ella en forma inmediata, evitando el acceso a esta información por personas no autorizadas.
- Las impresoras ubicadas en atención o tránsito de público deben estar protegidas de acceso no autorizado.
- Cuando sea posible y se trate de información sensible, debe implementarse el control de impresión con el uso de contraseña por parte del usuario.

5.4. Salas limpias.

- Las salas o áreas de reuniones, salas de conferencias y de capacitación, deben quedar limpias de todo el material utilizado.

5.5. Pizarras limpias

- Después de las reuniones en que se utilicen pizarras, estas deben quedar limpias de la información que se ha expuesto en ellas.
- En el caso de que se utilice un equipo computacional para presentaciones, si este fuera de uso común, debe eliminarse la información antes expuesta.

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	Nov. 2011	Versión inicial
02	Diciembre 2016	- Se modifican los revisores. - Se incorporan aspectos relacionados con la difusión y revisión de las políticas específicas.
03	Noviembre 2017	Se actualizan "Vistos", "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, de 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.



MIMV/MAG/AGG/PPP/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