Ministerio de Vivienda y Urbanismo

Gobierno de Chile

DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 14.494 (V. Y U.), DE 2017, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO, 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
30 DIC 2019
RESOLUCION EXENTA
TRAMITADA

SANTIAGO, 30 DIC 2019

RESOLUCIÓN EXENTA N° 3072/

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, 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 Control de Acceso Lógico, aprobada por Resolución Exenta N° 14.494, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

I. **Derógase** la Política Específica de Seguridad de control de acceso lógico, aprobada por Resolución Exenta 14.494, (V. y U.), de 2017.

II. **Apruébase** la Política Específica de Seguridad de la Información relativa a Control de Acceso Lógico, la que se detalla a continuación:

"POLÍTICA ESPECÍFICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO"

1. OBJETIVO

Esta política establece las definiciones que regulan el acceso a la información del MINVU, la que se encuentra administrada y confiada a ella.

2. ALCANCE

La presente Política, considerada como parte del Dominio de Control de Acceso, se aplica a toda la información que se encuentra en los sistemas computacionales del MINVU. 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

- Política específica de seguridad para el uso de las redes.
- Normativa de control de acceso.
- Normativa de gestión de logs de auditoría y registros de sistemas.

4. ROLES Y RESPONSABILIDADES

Encargado/a de Seguridad de la Información y Ciberseguridad

- Velar por el cumplimiento de la presenta política específica en la institución.

Jefe de División Informática

- Disponer los controles y reglas de control de acceso.

Usuarios líderes/Dueños de los Datos

- Definir los accesos a los datos por parte de los usuarios de la Institución y terceros, cuidando de mantener una adecuada segregación de funciones.
- Gestionar los accesos definidos.

Usuarios

- Cumplir con las definiciones establecidas en esta política.

5. REGLA DE LA POLITICA

5.1 Cumplimiento de la legislación

- Las medidas de control de acceso lógico definidas deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales.

5.2 Negación de acceso por omisión

- Los usuarios del MINVU solo deben tener acceso a la información que es necesaria para ejercer sus funciones.
- Estas necesidades de acceso deben ser determinadas por las respectivas jefaturas, en función de las tareas asignadas al cargo del funcionario.

5.3 Niveles de control de acceso

- El control de acceso debe ser administrado considerando las distintas instancias que un usuario debe resolver para tener acceso a los datos, esto es: redes, sistemas operativos, aplicaciones y bases de datos.

5.4 Administración del acceso

- La administración de perfiles radica en los Usuarios Líderes de Aplicación y las Jefaturas de División correspondientes. La responsabilidad de asignar un determinado perfil a un usuario corresponderá a la Jefatura de División solicitante o a quien delegue para esta función.
- Las decisiones de control de acceso que se toman deben ser consistentes con la clasificación de la información definida.
- Para facilitar la administración de los accesos, se deben definir perfiles de acceso asignables a grupos de usuarios que, por sus responsabilidades en la organización, presenten necesidades de acceso equivalentes.
- El Departamento de Ingeniería implementa las reglas de control de acceso solicitadas por los Usuarios Líderes de Aplicación y las Jefaturas de División correspondientes.

5.5 Administración de accesos especiales

- El otorgamiento de accesos con mayores privilegios, deben ser autorizados por la jefatura responsable, requiriendo el conocimiento y aprobación del Jefe de División Informática.

5.6 Segregación de funciones

- La asignación de atributos de acceso debe ser definida respecto a funcionarios individuales, de forma que la responsabilidad por las acciones ejercidas con los accesos otorgados sea directamente atribuible solo a él.
- El otorgamiento de accesos respecto a recursos de información del MINVU debe considerar una adecuada segregación de funciones, de modo que un mismo funcionario no pueda disponer, por su sola voluntad, del control de un proceso de negocios completo.
- Las excepciones a la regla anterior deben ser aprobadas por la Jefatura de División correspondiente y autorizadas por el jefe de la División de Informática.

5.7 Revocación de los accesos lógicos

- Ante la situación de un cambio de cargo de un funcionario, se deben revisar sus permisos de acceso lógico asignados y verificar que éstos sigan siendo válidos de acuerdo a su nueva función.
- Cuando un funcionario termina su relación laboral con el MINVU, todos sus permisos de acceso a la información deben ser revocados.
- Es responsabilidad de las Jefaturas Directas informar formalmente a la División Informática de estas situaciones, para proceder a revocar los accesos, lo cual será relevado a la División Administrativa para su validación.

5.8 Revocación de Accesos

- Los Usuarios Líderes de aplicación deben revisar en forma periódica los perfiles de usuario del personal vigente y solicitar a la División de Informática la actualización de éstos cada vez que ocurra un cambio en la definición de funciones.
- Los accesos de cuentas con mayores privilegios deben ser revisadas al menos 2 veces al año.

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 utilizar 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 debe evaluar 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 2015	Actualización del formato de la política
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; Agustin 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

MINISTERIO DE VIVIENDA Y URBANISMO

MMV/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