Ministerio de Vivienda y Urbanismo

Gobierno de Chile

APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD PARA LAS RELACIONES CON EL PROVEEDOR, 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
28 NOV 2019
RESOLUCION EXENTA TRAMITADA

SANTIAGO, 28 NOV 2019 HOY SE RESOLVIO LO QUE SIGUE

RESOLUCIÓN EXENTA N° 2690

VISTOS:

Lo dispuesto en el D.L N° 1305, de 1975, que reestructura y regionaliza el Ministerio de Vivienda y Urbanismo; 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 de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo; el Decreto Supremo N° 28, de 2018, que designa Subsecretario de Vivienda y Urbanismo; el Decreto Exento RA N° 272/58/2018, que establece orden de subrogación del cargo de Subsecretario de Vivienda y Urbanismo, todos del Ministerio de Vivienda y Urbanismo; 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. 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 Norma Chilena NCh-ISO 27.001 que proporciona un marco de gestión de Seguridad de la Información utilizable por cualquier tipo de organización, pública o privada.

b. La Resolución Exenta N° 2.097, (V. y U.), de 2019, que aprobó la Política General de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo.

c. Que resulta necesario establecer una Política Específica de Seguridad para las relaciones con el proveedor del MINVU, para reglamentar el acceso de proveedores externos a los activos de información, con el fin de proteger la confidencialidad, integridad y su disponibilidad dicto la siguiente:

RESOLUCIÓN:

I. **Apruébase** la Política Específica de Seguridad para las relaciones con el proveedor del MINVU, la que se detalla a continuación:

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

"POLÍTICA ESPECÍFICA DE SEGURIDAD PARA LAS RELACIONES CON EL PROVEEDOR DEL MINVU"

1. OBJETIVO

Se establece la siguiente política con el objeto de indicar las reglas para la contratación de servicios externos, asociados al acceso de proveedores a los activos de información del MINVU, incluido todo el personal externo que trabaja en el Servicio y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información.

2. ALCANCE

La presente Política, es aplicable a toda relación con terceros realizada por un proceso de compra en la Subsecretaria de Vivienda y Urbanismo Nivel Central y sus 16 Secretarias Regionales Ministeriales, que involucre el acceso, procesamiento y/o comunicación de los activos de información relevantes de la institución. Se excepcionará aquellas contrataciones que, por su relevancia e imposibilidad real de negociación, deban realizarse necesariamente mediante la suscripción de contratos de adhesión, en las que se deban aceptar las cláusulas propuestas.

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 cual se manifieste tal voluntad.

Esta política contempla los requisitos del control A.15.01.01 Política de seguridad de la información para las relaciones con el proveedor, definido en la Norma NCH-ISO 27001:2013 Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información, cuyo objetivo plantea acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización.

3. DOCUMENTOS RELACIONADOS

- Ley N° 19.886, Ley de Bases sobre Contratos Administrativos de Suministros y Prestación de Servicios.
- DS N° 250 de 2004 de Hacienda, Reglamento Ley de Compras.
- Decreto Supremo N°83, de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Norma chilena NCh-ISO 27001 (INN), sobre Sistema de Gestión de la Seguridad de la Información – requisitos.
- Norma chilena NCh-ISO 27002 (INN), sobre Tecnología de la Información – Código de prácticas para la gestión de seguridad de la información.
- Manual de procedimientos del sistema de compras y contrataciones del Ministerio de Vivienda y Urbanismo y sus Secretarías Regionales Ministeriales.
- Política General de Seguridad de la Información y Políticas Específicas.
- Política de Correo electrónico.
- Política Específica de Uso de Red Informática.
- Política Específica de Control de Cambio.
- Política Específica de Cuentas de Usuario.
- Política Específica de Desarrollo de Sistemas.
- Política Específica de Identificación y Autenticidad.
- Política Específica de Intercambio de información con terceros.
- Política Específica de Mensajería Instantánea.
- Política Específica de Seguridad de Protección Contra Código Malicioso.
- Política Específica de Seguridad en uso de Controles Criptográficos.
- Política Específica de Seguridad de Control de Acceso Físico.
- Política Específica de Seguridad de Control de Acceso Lógico.

- Política Específica de Seguridad de Medios Removibles.
- Política Específica de Seguridad de Pantallas y Escritorios Limpios.
- Política Específica de Seguridad de Redes.
- Política Específica de Seguridad de Respaldo y Retención de Información.
- Política Específica de Seguridad de Uso de Equipos y Comunicaciones móviles.
- Política Específica de Seguridad en Uso de Computadores del MINVU.
- Política Específica de Uso de las Contraseñas.
- Política Navegación internet.
- Política Uso de Software.

4. ROLES Y RESPONSABILIDADES

Jefe de Departamento de Compras y Servicios Generales y en las SEREMI, quien determine el Secretario Regional Ministerial

- Velar por el cumplimiento de la siguiente política.
- Dar cumplimiento a lo establecido en el Manual de Compras.
- Velar por la inclusión de las cláusulas de confidencialidad de la información, propiedad intelectual y seguridad de la información en contratos con terceros, cuando corresponda.

Proveedores

- Dar estricto cumplimiento a las normas de seguridad de la información descritas en la presente política. Esta obligación también es aplicable a los subcontratos en caso de que ello ocurra.

Personal Externo que preste servicios al MINVU

- Dar estricto cumplimiento a las normas de seguridad de la información descritas en la presente política.

Usuarios Internos:

- Todos los usuarios internos que interactúan con el personal de los proveedores deben dar estricto cumplimiento a la reglamentación existente respecto al acceso del proveedor a los sistemas y la información de la organización.

Encargado de Seguridad de la Información y en las SEREMI, quien determine el Secretario Regional Ministerial

- Velar por el cumplimiento de esta política.

5. REGLAS DE LA POLÍTICA

Cuando el MINVU establezca relaciones con proveedores que impliquen el acceso de estos a los activos de información, se debe incorporar cuando sea pertinente, en las bases de licitación pública, términos de referencia, invitaciones a procesos de Grandes Compras y solicitudes de cotización para contrataciones realizadas a través de convenio marco, cláusulas relativas a la seguridad de la información, confidencialidad, propiedad intelectual, integridad de la información a la que tienen acceso personas externas al MINVU y posteriormente, realizar un seguimiento de que éstos cumplen con los acuerdos definidos, aplicando estas directrices:

5.1. Consideraciones generales para cumplimiento de la Política General de Seguridad de la información.

a) Todo el personal externo que desarrolle labores para el Minvu deberá tomar conocimiento de la Política General de Seguridad de la Información, observando sus directrices y colaborando en su aplicación dentro de su ámbito de acción.
b) Para estos efectos, el trabajo o proyecto realizado por el proveedor debe ser compatible con los estándares de seguridad de la información establecidos.

5.2. Prestación de Servicios en el MINVU

a) Los proveedores solo podrán desarrollar para el MINVU aquellas actividades cubiertas bajo el correspondiente contrato y de acuerdo a lo establecido en las respectivas bases y contrato de prestación de servicios.

b) La empresa proveedora deberá asegurar que su personal que presta servicios en el MINVU, tiene la formación y capacitaciones requeridas para efectuar el trabajo contratado.

5.3. Confidencialidad de la Información

a) El personal externo que tenga acceso a información de MINVU deberá entender que dicha información tiene carácter de confidencial.
b) Queda prohibido para los proveedores revelar, modificar, destruir o dar mal uso de la información, cualquiera que sea el soporte en el cual está contenida.
c) El proveedor deberá resguardar por un tiempo indefinido la confidencialidad y no podrá difundir la información a la que se tiene acceso, salvo que esté debidamente autorizado por el MINVU.
d) En caso que, por motivos directamente relacionados con el trabajo, el empleado de la empresa proveedora tome conocimiento de información confidencial contenida en cualquier tipo de soporte, deberá entender que es estrictamente temporal, con obligación de secreto y sin que con ellos se le confiera derecho de posesión, titularidad o copia de la citada información.
e) Cada vez que un proveedor requiera información adicional a aquella que el MINVU ha entregado en virtud del respectivo contrato, el propietario de la información debe analizar los motivos de dicho requerimiento y proceder a la aprobación o rechazo a la entrega de la misma.

5.4. Propiedad Intelectual

a) Todo el personal externo deberá garantizar el cumplimiento de las restricciones legales de uso del material protegido por normas de propiedad intelectual.
b) Al personal externo les queda estrictamente prohibido el uso de programas informáticos que no cuenten con licencia original y vigente.
c) Al personal externo les queda prohibido el uso, reproducción, cesión, trasformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.

5.5. Se prohíbe expresamente al personal externo:

a) La comercialización o entrega de información de propiedad del MINVU, o bases de datos de usuarios, personal y/o proveedores.
b) El uso de los recursos proporcionados por el MINVU para actividades no relacionadas con el propósito del servicio.
c) Introducir en los sistemas de información o red contenidos obscenos, amenazadores, inmorales u ofensivos.
d) Introducir voluntariamente a la red cualquier tipo de malware (programas, macros, otro), dispositivo lógico, dispositivo físico o cualquier otro tipo de consecuencias de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Todo personal con acceso a la red tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los sistemas de elementos destinados a destruir o corromper los datos informáticos.
e) Obtener sin autorización otros derechos o accesos que el dueño del sistema le haya asignado.
f) Acceder sin autorización del MINVU a áreas restringidas de los sistemas de información.
g) Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, dañar o alterar los recursos informáticos del MINVU.
h) Destruir, alterar, inutilizar o efectuar cualquiera otra forma de dañar datos, programas o documentos electrónicos de responsabilidad y custodia del MINVU.

5.6. Responsabilidad del proveedor

a) Las personas con acceso a la información del MINVU son responsables de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive.
b) Los usuarios no deberán utilizar ningún identificador distinto al propio, aunque disponga de la autorización del propietario.

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

c) Los proveedores de servicio deberán asegurarse de que todo el personal que desarrolla labores para el MINVU, respete las condiciones establecidas en la respectiva Política Específica.

La aplicación de las cláusulas de seguridad en los contratos administrativos, bases de licitación, tratos directos, actos administrativos o cualquier otro documento formal relacionado con la contratación de servicios a proveedores, será responsabilidad de la Jefatura del Departamento de Compras y Servicios Generales y en las SEREMI, quien determine el Secretario Regional Ministerial.

6. Actuación ante eventos e incidentes

En la eventualidad de ocurrir algún incidente de seguridad de la información relativo a las medidas de seguridad indicadas en esta política, la(s) persona(s) que lo detecte(n) debe(n) informar a la brevedad a su contraparte MINVU, quienes analizarán y canalizarán el incidente, para luego tomar las medidas necesarias para minimizar los potenciales daños a los activos de información definidos por MINVU, previniendo la ocurrencia de incidentes y así, dar cumplimiento a esta política, de acuerdo a los procedimientos internos / procedimiento gestión de incidentes.

7. DIFUSIÓN

La comunicación y difusión de la presente política específica es responsabilidad de cada Encargado/a de Seguridad de la Información o en quien designe esta función, pudiendo utilizar para ello los canales de difusión establecidos, como publicación en la Intranet institucional y/o Minvuletín y/o Correo electrónico y/o Afiches y/o 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. 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.

9. CONTROL DE VERSIONES

N° Versión	Fecha Aprobación	Motivo de la revisión
01	Septiembre 2019	Versión Inicial

Elaborado por:
Emilia Bustamante Ibarra, Jefe Departamento de Compras y Servicios Generales, División Administrativa; Anita Ide Vilugron, Analista Jurídico Departamento de Compras y Servicios Generales, División Administrativa; Francisco Javier Solis Romero, Encargado Sección Gestión de Abastecimiento de Departamento de Compras y Servicios Generales, División Administrativa; Ivonne Valdivia Galindo, Analista Departamento Estudios, División Administrativa; Sandra Rivera Santana/ Jefa Departamento Soporte Tecnológico a la Gestión, División de Informática; Leonardo Cavieres Córdoba/ Encargado de Seguridad Informática, División de Informática; Claudio Paredes Pizarro/ Encargado de Sección de Ingeniería y Explotación de Sistemas, División

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

de Informática; Juan Pablo Ríos/ Abogado, División Jurídica; Marcela Jara Cartes, Analista Departamento de Planificación y Control de Gestión, División Finanzas.

Revisado por:
Marcela Acuña Gomez, Encargada de Seguridad de la Información; Agustín Goñi Gonzalez, Jefe División de Informática; Claudia Ernst Valencia, Jefe División Administrativa.

II. **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.

III. **Realícense** por el Jefe de la División Administrativa, Jefe División de Informática y el Encargado de Seguridad del MINVU y en las SEREMI, quien determine el Secretario Regional Ministerial, las acciones tendientes a su implementación en materias de su competencia.

IV. 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

MAG/GEA/AGG/ACA/CEV/AUE/CPP/MJC/EBI/IVG/JPR/FSR/AIV

DISTRIBUCIÓN:
- Gabinete Ministro V. y U.
- Gabinete Subsecretario V. y U.
- SEREMI (16)
- Divisiones Nivel Central (7)
- Departamento de 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

647

FIEL DO QUE TRANSCRIBO PARA SU CONOCIMIENTO

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

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA