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°14.486, (V. Y U.), DE 2017, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO, EN EL MARCO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO.

30 DIC 2019

SANTIAGO, HOY SE RESOLVIO LO QUE SIGUE

3097

RESOLUCIÓN EXENTA N° _____/

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 Norma Chilena 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 Protección contra Código Malicioso, aprobada por Resolución Exenta N° 14.486, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

I. **Derógase** la Política Específica de Seguridad de protección contra código malicioso aprobada por Resolución Exenta 14.486, (V. y U.) de 2017.

II. **Apruébase** la Política Específica de Seguridad de la Información, relativa a la protección contra código malicioso, la que se detalla a continuación:

"POLÍTICA DE SEGURIDAD PROTECCIÓN CONTRA CÓDIGO MALICIOSO"

1. OBJETIVO

Esta política establece las reglas que permiten gestionar los eventos relacionados con virus, troyanos, gusanos y otros tipos de códigos maliciosos, tanto a nivel de la red, estaciones de trabajo como también de aplicaciones.

2. ALCANCE

La presente Política considerada como parte del Dominio de Seguridad de las Operaciones y se aplica a la protección de la red, servidores y estaciones de trabajo, sean estacionarias o portátiles, locales o remotas, así como también las aplicaciones desarrolladas tanto interna como externas. 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.12.02.01 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 de uso de Software.
- Política específica de desarrollo de sistemas
- Normativa de gestión de antivirus.

4. ROLES Y RESPONSABILIDADES

Encargado/a de Seguridad de la Información y ciberseguridad

- Velar por el cumplimiento de esta política.
- Gestionar los incidentes de seguridad por software malicioso.
- Concientizar a los usuarios de los posibles riesgos en el uso de la internet y correo Institucional.

Jefe de División Informática

- Proveer los medios para administrar la plataforma antivirus y controlar el desarrollo de las aplicaciones de MINVU.
- Validar y autorizar la instalación de herramientas de detección de códigos malicioso.

Sección Ingeniería y Explotación de Sistemas - Área de Redes y Sistemas- División de Informática

- Disponer de medidas de protección adecuadas para la prevención de códigos maliciosos.
- Controlar las aplicaciones de Minvu, respecto a posible inyección de código malicioso.
- Revisar que los clientes del antivirus se encuentren debidamente actualizados.

Departamento de Soporte Tecnológico a la Gestión- División de Informática

- Recibir y canalizar cualquier aviso de un incidente por código malicioso.
- Gestionar los eventos por código malicioso producidos.
- Revisar que los clientes del antivirus se encuentren debidamente actualizados.

Coordinadores informáticos regionales

- Recibir y canalizar cualquier aviso de un incidente por código malicioso.

- Gestionar los eventos por código malicioso producidos.
- Revisar que los clientes del antivirus se encuentren debidamente actualizados.

Usuarios

- Reportar cualquier incidente que signifique la presencia o presunción de presencia de código malicioso.
- Mantener la configuración de su estación de trabajo, estandarizada por el área de Informática.
- Cumplir con las reglas y prohibiciones establecida en este documento.

5. REGLAS DE LA POLÍTICA

5.1. Definición inicial

- La Jefatura de División Informática debe definir formalmente el(los) software(s) estándar apropiado (s), para el apoyo en la detección y contención de códigos maliciosos.

5.2. Protección de código malicioso a nivel de red

- MINVU debe contar con un servicio centralizado que permita verificar la presencia de código malicioso en todos sus servidores. De la misma forma, se debe contar con herramientas adecuadas de control de presencia de código malicioso para los servicios de Navegación Internet, de Mensajería de correos electrónicos entrantes y salientes.

5.3. Protección en estaciones de trabajo

- Toda estación de trabajo debe contar con un producto de protección contra código malicioso instalado y permanentemente actualizado, tanto en su versión de software como en los respectivos patrones de búsqueda. Para ello se debe establecer un proceso centralizado y automático, además de un mecanismo alternativo manual, el que será utilizado cuando el proceso automático no pueda ejecutarse. La configuración de este servicio debe cumplir con los siguientes requisitos:
- Se active siempre y permanezca activo.
- Revise en forma automática cualquier medio de almacenamiento removible que se intente utilizar en la estación de trabajo.
- Que la notificación ante la detección de un código malicioso sea notificada automáticamente al Departamento de Ingeniería.

5.4. Protección en aplicaciones desarrolladas

- Toda aplicación que es publicada hacia internet, desarrollada o mantenida, tanto en forma interna como externa, debe ser controlada para asegurar que no contiene código malicioso.

5.5. Gestión de actualización y alertas

- La administración de este tipo de software debe estar suscrita a un servicio de alertas y actualización, como también de sus respectivos patrones.

- Se debe actualizar el producto de protección contra código malicioso cada vez que el fabricante provea nuevas versiones.

- El Departamento de Ingeniería debe estar preparado para ejecutar actualizaciones de emergencia.

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 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

N° Versión	Fecha Aprobación	Motivo de la revisión
1	Noviembre 2012	Versión inicial
2	Diciembre 2016	- Se modifican los revisores. - Se incorporan aspectos relacionados con la difusión y revisión de las políticas específicas. - Se incluyen las normativas asociadas a esta política.
3	Noviembre 2017	Se actualizan "Considerando" y "Objetivo
4	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 González/ 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

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

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

MIMV/MAG/AGG/CPP/ECC

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