Ministerio de Vivienda y Urbanismo

Gobierno de Chile

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA
21 DIC 2017
RESOLUCION EXENTA
TRAMITADA

DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 10.377, (V. Y U.), DE 2015, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE INFORMACIÓN DE PROTECCIÓN CLAVE DE CIFRADO DE USUARIO FINAL, EN EL MARCO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO.

SANTIAGO, 21 DIC 2017

RESOLUCIÓN EXENTA N° 014496 /

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 2005, 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° 13.453, (V. y U.), de 2017, que aprueba la Política de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo; la Resolución N° 1600 de 2008, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón; y

CONSIDERANDO:

a. Que se han dictado una serie de normas entre las que se encuentra el Decreto Supremo N° 83, de 2005, 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° 13.453, (V. y U.), de 2017, se ha aprobado una nueva política general de seguridad de la información para el Ministerio de Vivienda y Urbanismo.

c. Que 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 Información de Protección Clave de Cifrado de Usuario Final aprobada por Resolución Exenta 10.377, (V. y U.), de 2015, motivo por el cual dicto la siguiente:

RESOLUCIÓN:

I. **Deróguese** la Política Específica de Seguridad de Información de Protección Clave de Cifrado de Usuario Final aprobada por Resolución Exenta 10.377, (V. y U.), de 2015.

II. **Apruébese** la Política Específica de Seguridad de Información de Protección Clave de Cifrado de Usuario Final, la que se detalla a continuación:

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

"POLÍTICA ESPECÍFICA DE SEGURIDAD DE INFORMACIÓN DE PROTECCIÓN CLAVE DE CIFRADO DE USUARIO FINAL"

1. OBJETIVO

Esta política describe los requisitos para la protección de claves de cifrado que están bajo el control final de los usuarios. Estos requisitos son diseñados para evitar divulgación no autorizada y posterior usos fraudulentos. Los métodos de protección descritos incluyen controles operacionales y técnicos, como procedimientos de copia de la clave de seguridad y uso de hardware especializado.

2. ALCANCE

La presente Política considerada como parte del Dominio de Control de Acceso y Dominio de Criptografía, se aplica a cualquier clave de cifrado emitida por el Ministerio o emitida para proteger datos de propiedad del Ministerio y a la persona responsable de ella.

Esta política debe ser cumplida por 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 manifiesta tal voluntad.

3. DOCUMENTOS RELACIONADOS

- Política específica de seguridad de aceptación de firma electrónica
- Política específica de administración de claves

4. ROLES Y RESPONSABILIDADES

Comité de Seguridad de la Información

- Definir los controles necesarios para el control de la administración de las claves durante su ciclo de vida.
- Monitorear la política en cuestión

Encargado de Seguridad de la Información

- Apoyar al Comité de Seguridad de la Información de la Institución en la definición de los controles de administración de las claves
- Validar que los controles de administración definidos cumplen con las necesidades de la Institución y se encuentren ajustadas a Derecho.

Jefe de Sección Ingeniería y Explotación de Sistemas de la División de Informática

- Administrar las claves criptográficas.

Personal de la División Informática

- Utilizar solo los controles de protección del ciclo de vida de las claves autorizadas por la Institución.

Unidades de la Institución

- Cautelar el cumplimiento de las medidas de control del uso de controles de la administración de claves.
- Reportar supuestas violaciones de seguridad en el ciclo de vida de las claves.

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN CARLOS RÍOS
Abogado
DIVISIÓN JURÍDICA

5. REGLAS DE LA POLÍTICA

5.1 Marco de referencia

- Se debe cifrar toda información sensible, clasificada como de riesgo alto, que pudiese quedar expuesta a usuarios no autorizados, en relación a su privacidad e integridad.
- Se utilizarán controles de cifrado para la protección de la confidencialidad, el cumplimiento del principio de la no-repudiación y el control de la integridad de la información.

5.2 Marco General

- Todas las claves de cifrado cubiertas por esta política son protegidas para evitar su divulgación no autorizada y posterior uso fraudulento.
- Para lo anterior las distintas claves de usuario se clasificarán en claves de cifrado de claves secretas, y Claves de Cifrado Público PKI (Infraestructura de Claves Públicas) del Ministerio.

5.3 Claves de cifrado de clave secreta

- Las claves de usuario de propósito general utilizaran un solo factor de autenticación.
- Para intercambiar claves simétricas, se deben utilizar métodos de cifrado.

5.4 Claves de Cifrado Público PKI (Infraestructura de Claves Públicas) del Ministerio

- La Firma electrónica avanzada cumple con los aspectos de protección según la Ley N°19.799 de Firma Electrónica aplicada a Organismo del Estado, siendo MINVU perteneciente a tal categoría.
- Los pares de claves pública-privada utilizados en el Ministerio se generan en un token a prueba de manipulaciones emitida a un usuario final individual acorde a la ley N°19.799. La clave privada asociada con el certificado de identidad de un usuario final, que sólo se utiliza para firmas digitales, nunca abandonará el token. La clave privada asociada a cualquier certificado de cifrado, que se utiliza para cifrar correo electrónico y otros documentos, son almacenadas en cumplimiento con la política del Ministerio.
- El acceso a las claves privadas almacenadas en un token, emitidas para funcionarios del Ministerio estará protegido por un número de identificación personal (PIN) conocido solamente por la persona a quien se le asigne el token. El software del token autorizado por el Ministerio estará configurado para requerir ingresar el PIN antes de cualquier uso de él.

5.5 Almacenamiento en Token

- Las claves cifradas almacenadas en el Token serán tratadas como un equipo del Ministerio con información sensible, de acuerdo a la Política de Seguridad Física. Además, los token, no deberán estar conectados al computador del usuario cuando no esté en uso.

5.6 PIN (número de identificación personal), claves

- Todos los PIN y contraseñas utilizadas para proteger las claves de cifrado deben cumplir con requisitos de complejidad y longitud que se describe en la Política de contraseñas.

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN MARIO RÍOS
Abogado
DIVISIÓN JURÍDICA

5.7 Pérdida o Robo

- La pérdida, robo, o potencial divulgación no autorizada de cualquier clave de cifrado cubierta por esta política serán reportados inmediatamente según el procedimiento de gestión de incidentes de seguridad y se procederá a la revocación del certificado y que el usuario solicite la emisión de uno nuevo.
- En caso de revocación de algún certificado de firma electrónica, se notificará de esta acción al titular de dicho certificado.
- El Encargado de Seguridad de la Información debe ser informado inmediatamente en caso que se reciba cualquier comunicado (por teléfono, correo postal o correo electrónico) de parte de una autoridad de protección de datos u otro ente regulador.

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 designe esta función, pudiendo utilizar para ello los canales de difusión establecidos, como Intranet, correo electrónico, Minvuletín, entre otros. Adicionalmente, las Políticas específicas se encuentran publicadas en la página web del MINVU en el banner Ministerio/Gestión Ministerial.

7. 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 Aprobació	Motivo de la revisión
01	Diciembre 2015	Versión inicial
02	Noviembre 2017	Se actualizan "Considerando" y "Objetivo"

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; Marcela Jara Cartes/ Encargada Sección Gestión de Procesos Depto. Planificación y Control de Gestión, División Finanzas.

Revisado por:
Alexia Naranjo Loyola, Encargada de Seguridad de la Información; Yelka Ruiz Rocha/ Jefa División de Informática.

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA

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 la Jefa 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
SUBSECRETARIA

JOCELYN FIGUEROA YOUSEF
SUBSECRETARIO DE VIVIENDA Y URBANISMO (S)

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

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

ANL/YRR/CPP/LCC
DISTRIBUCIÓN:
- Gabinete Ministra V. y U.
- Gabinete Subsecretario V. y U.
- SEREMI (15)
- Divisiones Nivel Central (7)
- Auditoría Interna Ministerial
- Contraloría Interna Ministerial
- Coordinador Nacional Programa Reconstrucción
- Programa Aldeas y Campamentos
- 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

MINISTERIO DE VIVIENDA Y URBANISMO
M. CECILIA CÁCERES
Jefa
DIVISIÓN JURÍDICA

MINISTERIO DE VIVIENDA Y URBANISMO
JUAN PABLO RÍOS
Abogado
DIVISIÓN JURÍDICA