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° 14.478, 14.498, 14.497 y 14.496 (V. Y U.), DE 2017, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE USO DE CONTROLES CRIPTOGRAFICOS, EN EL MARCO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO.

SANTIAGO, 30 DIC 2019

RESOLUCIÓN EXENTA N° 3075

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 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 Uso de Controles Criptográficos aprobada por Resolución Exenta 14.481, (V. y U.), de 2017, Política Específica de Seguridad de aceptación de firma electrónica aprobada por Resolución Exenta 14.498, (V. y U.), de 2017, Política Específica de Seguridad de Administración de Claves aprobada por Resolución Exenta 14.497, (V. y U.), de 2017 y Política Específica de seguridad de información de protección clave de cifrado de usuario final aprobada por Resolución Exenta 14.496, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

I. **Derógase** la Política Específica de Seguridad de Uso de Controles Criptográficos aprobada por Resolución Exenta 14.481, (V. y U.), de 2017.

II. **Derógase** la Política Específica de Seguridad de aceptación de firma electrónica aprobada por Resolución Exenta 14.498, (V. y U.), de 2017.

III. **Derógase** la Política Específica de Seguridad de Administración de Claves aprobada por Resolución Exenta 14.497, (V. y U.), de 2017.

IV. **Deróguese** la Política Específica de seguridad de información de protección clave de cifrado de usuario final aprobada por Resolución Exenta 14.496, (V. y U.), de 2017.

V. **Apruébese** la Política Específica de Seguridad de uso de controles criptográficos, la que se detalla a continuación:

"POLÍTICA ESPECÍFICA DE SEGURIDAD DE USO DE CONTROLES CRIPTOGRÁFICOS"

1. OBJETIVO

Esta política tiene como objetivo establecer reglas que permitan hacer uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y la integridad de la información.

2. ALCANCE

La presente Política considerada como parte del Dominio de Criptografía, y 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 manifiesta tal voluntad.
Esta política está relacionada con el cumplimiento del control A.10.01.01 y A.10.01.02 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
- Normativa de gestión de Infraestructura de TI

4. ROLES Y RESPONSABILIDADES

Encargado/a de Seguridad de la Información y Ciberseguridad

- Velar por el cumplimiento y revisión de las Políticas basada en requisitos de negocio y seguridad de la información.

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

- Autorizar formalmente los métodos de encriptación a utilizar en las aplicaciones y sistemas tecnológicos.
- Generar e implementar los controles definidos en los procesos que afectan el control del uso de controles criptográficos.
- Administrar las claves criptográficas.

Personal de la División Informática

- Utilizar solo las claves criptográficas autorizadas por la Institución.
- Reportar supuestas violaciones de seguridad en el ciclo de vida de las claves criptográficas.

Usuarios

- Usar sólo herramientas de software provistas y autorizadas por el MINVU
- Reportar supuestas violaciones de seguridad en el ciclo de vida de las claves criptográficas.

5. REGLAS DE LA POLÍTICA

5.1 Marco de referencia para la criptografía

- Se deberá cifrar toda la información clasificada como restringida, que pudiese quedar expuesta para usuarios no autorizados.
- 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 Requisitos de los algoritmos y funciones de cifrado

- Para encriptación simétrica o de clave secreta donde se utiliza una clave única para encriptar y des encriptar mensajes solo se deberán utilizar algoritmos de cifrado "AES-compatibles".
- Para encriptación asimétrica o de clave pública como es el caso de la firma electrónica se deberá utilizar los algoritmos de cifrado basados en curvas elípticas (ECDSA) o RSA equivalente.
- La Institución adhiere al uso de las funciones basadas en SHA-2.
- Todos los servidores utilizados para la autenticación deben contener un certificado válido firmado por un proveedor de confianza conocido.

5.3 Acerca del uso de la firma electrónica

- Para todo efecto el uso de la firma electrónica en el Minvu se basa en establecido en la Ley 19.799 referente a Documento Electrónico; Servicios de Certificación de Firma Electrónica.
- Para firma electrónica avanzada se utilizará un e-token (similar a pendrive) el cual contendrá un certificado digital que será asignado a los funcionarios que lo requieran previa validación.
- Para firmar documentos electrónicos el Minvu empleará firma electrónica avanzada.
- Para la firma electrónica avanzada solo se utilizará software aprobado por la División de Informática del Minvu.
- No se considerará confiable un documento electrónico firmado cuya firma no parezca válida.

5.4 Administración de las claves criptográficas

- Las claves criptográficas deben ser generadas y almacenadas en forma segura de manera tal que se evite el robo, perdida o compromiso de estas.
- Todas las claves criptográficas son protegidas contra divulgación, modificación y destrucción.
- Se proveerá de protección física al equipamiento utilizado para generación, almacenamiento de claves criptográficas, considerando los respaldos correspondientes y el resguardo y protección de accesos a éstas.
- Para intercambiar claves simétricas se deben utilizar métodos de cifrado.
- Los firmantes protegerán su clave privada y la mantendrán en secreto
- No debe compartir ni delegar la firma electrónica a terceras personas dado que es de carácter personal e intransferible.
- Las claves privadas de los certificados digitales contenidos en los dispositivos e-token, serán protegidos mediante un PIN (número de identificación personal) y solo debe ser conocido por el propietario de dicho certificado digital.
- Las claves privadas almacenadas en los e-token serán gestionadas como un activo propiedad de la institución.
- Ante pérdida o robo de un e-token que contiene un certificado digital se debe informar a la mesa de atención de usuarios del nivel central para proceder con la revocación del certificado asignado contenido en el e-token

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 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 Aprobó.	Motivo de la revisión
01	Diciembre 2015	- 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	- Actualización de referencias de los "Vistos" se agregan reglas, cambios a las reglas y a las prohibiciones de política
04	Noviembre 2019	- Se actualiza resolución de la nueva política general de seguridad de la información, se modifica el 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 velar por su estricto cumplimiento.

IV. **Realícense** por el 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

MIMV/MAG/AGG/CPP/LCC

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

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

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