Ministerio de Vivienda y Urbanismo

Gobierno de Chile

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA
06 OCT 2020
RESOLUCION EXENTA
TRAMITADA

COMPLEMENTA RESOLUCIÓN EXENTA N° 3092, (V. Y U.), DE 2019 QUE APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE ACCESO A LAS REDES Y A LOS SERVICIOS DE LA RED, EN EL MARCO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO, EN EL SENTIDO QUE INDICA.

SANTIAGO, 06 OCT 2020 HOY SE RESOLVIO LO QUE SIGUE

RESOLUCIÓN EXENTA N° 01447 /

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 acceso a las redes y a los servicios de la red, aprobada por Resolución Exenta N° 3092, (V. y U.), de 2019, en cuanto a agregar y regular aspectos asociados al teletrabajo, redes virtuales privadas (VPN) y a redes inalámbricas (WIFI).

e. La necesidad de mantener operativo y en pleno funcionamiento la modalidad de trabajo a distancia, para lo cual se hace necesario regular las redes virtuales privadas (VPN), dicto la siguiente:

RESOLUCIÓN:

I. **Compleméntase** la Política Específica de Seguridad de acceso a las redes y a los servicios de la red, aprobada por Resolución Exenta N° 3092, (V. y U.), de 2019 en el siguiente sentido:

1. **Reemplázase** el punto 5.3 "Manejo de conexiones externas", por el siguiente:

5.3 **"Manejo de conexiones externas**

- El Minvu implementará una red privada virtual (en adelante VPN) institucional.
- Los accesos vía VPN deben considerar una vigencia de uso.
- Los funcionarios deberán acceder a la modalidad de teletrabajo mediante el uso de la VPN institucional.
- Los accesos para los funcionarios que requieran VPN deberán ser gestionados por su jefatura directa. Esto incluye la solicitud de acceso inicial, de extensión de vigencia o la solicitud de caducar el acceso en forma previa a la fecha de vigencia inicial, según corresponda.
- Toda solicitud de acceso externo especial debe ser solicitada al Jefe de División Informática, quien podrá aceptarla o rechazarla, la cual debe indicar el motivo de la solicitud, los sistemas o servicios de los cuales se requiere el acceso, periodo de vigencia y la información de identificación del solicitante.
- Todas las conexiones externas deben ser registradas y monitoreadas.
- Cada conexión con entidades externa debe tener definida previamente su nivel de confianza y los controles asociados para garantizar la seguridad del intercambio de datos.
- El Encargado de Seguridad de la Información y Ciberseguridad es responsable de establecer revisiones periódicas de cumplimiento de los controles definidos, independiente de las revisiones efectuadas por personal de la División de Informática."

2. **Intercálase** el siguiento punto 5.8, pasando el actual punto 5.8 a ser el nuevo punto 5.9:

5.8 "Acerca del uso de las redes inalámbricas (WIFI) del Minvu.

- El Minvu proveerá una solución para redes inalámbricas institucional cuya cobertura está condicionada a los recursos disponibles.
- El Minvu proveerá una red inalámbrica institucional que no reemplaza a la red fija, es considerado un método alternativo de acceso.
- Se habilitarán dos modalidades de acceso a red institucional inalámbrica, una para funcionarios y otra para invitados.
- La División de informática de la subsecretaría será la encargada de proveer el servicio de red inalámbrica institucional a nivel nacional en coordinación con los Servicios de Vivienda y Urbanización y las Secretarias Regionales cuando corresponda.
- No se deberán implementar soluciones de redes inalámbricas alternativas o complementarias en la red del Minvu."

II. **Establécese** la obligación del Encargado/a de Seguridad de la Información y Ciberseguridad de la Subsecretaría de difundir la política aprobada por la Resolución Exenta N° 3092, (V. y U.), de 2019, y su complementación aprobada en este acto, y en coordinación con el Comité de Seguridad de la Información velar por su estricto cumplimiento.

III. Realícense por el Jefe de la División de Informática 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

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

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

MIMV/MAG/MANM/LCC

DISTRIBUCIÓN:

- Gabinete Ministro V. y U.
- Gabinete Subsecretario V. y U.
- SEREMI (16)
- SERVIU (16)
- Divisiones Nivel Central (7)
- 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
- Centro de Estudios Ciudad y Territorio
- Depto. Planificación y Control de Gestión DIFIN
- Oficina de Partes

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° 14.477, (V. Y U.), DE 2017, Y RESOLUCIÓN EXENTA N°14.485, (V. Y U.), DE 2017, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE ACCESO A LAS REDES Y A LOS SERVICIOS DE LA RED, EN EL MARCO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO.

SANTIAGO, 30 DIC 2019 HOY SE RESOLVIO LO QUE SIGUE

RESOLUCIÓN EXENTA N° 3092 /

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 uso de red informática aprobada por Resolución Exenta 14.477, (V. y U.), de 2017, y la Política Específica de seguridad de uso de redes aprobada por Resolución Exenta 14.485, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

I. **Derógase** la Política Específica de Seguridad de Uso de red informática, aprobada por Resolución Exenta 14.477, (V. y U.), de 2017 y Política Específica de Seguridad de uso de redes, aprobada por Resolución Exenta 14.485, (V. y U.), de 2017.

II. **Apruébase** Política Específica de seguridad de acceso a las redes y a los servicios de la red, la que se detalla a continuación:

"POLITICA ESPECIFICA DE SEGURIDAD DE ACCESO A LAS REDES Y A LOS SERVICIOS DE LA RED"

1. OBJETIVO

Esta política define las reglas para el control de acceso a las redes y a los servicios de red del MINVU, mediante un conjunto de reglas que permitan utilizar el recurso de red de manera eficiente y responsable.

2. ALCANCE

La presente Política considerada como parte del Dominio de Control de Acceso, se aplica a las redes y servicios de red a los cuales es permitido acceder. 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.

3. DOCUMENTOS RELACIONADOS.

- Política de Seguridad de Control de acceso lógico
- Normativa de Gestión de Control de Acceso

4. ROLES Y RESPONSABILIDADES.

Jefe de División Informática

- Disponer los controles y reglas de control de acceso a las redes y a los servicios de red

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.

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.

Usuarios

- Cumplir con las definiciones establecidas en esta política

5. REGLAS DE LA POLÍTICA.

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 las redes y a los servicios a las redes que son necesarios 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. Manejo de conexiones externas

- Toda solicitud de conexión externa debe ser formalizada y aprobada por el Jefe de División Informática, indicando el motivo de la solicitud, los sistemas a los que accederá, periodo de conexión y la información de identificación del solicitante.
- Cada conexión con entidades externa debe tener definida previamente su nivel de confianza y los controles asociados para garantizar la seguridad del intercambio de datos.
- Todas las conexiones externas deben ser registradas y monitoreadas, mediante procesos definidos por la Sección de Ingeniería.
- El Encargado de Seguridad de la Información y Ciberseguridad es responsable de establecer revisiones periódicas de cumplimiento de los controles definidos, independiente de las revisiones efectuadas por personal de la, División de Informática

5.4. Sobre la seguridad en los servicios de red

- Se debe garantizar la disponibilidad de los servicios de red, acorde a las necesidades de MINVU.
- Se debe mantener el mapa de la topología de las redes actualizado, que contemple todos los elementos que componen la red de la organización, incluyendo si existen entornos críticos, conexiones con terceros, conexiones con internet, conexiones con regiones y accesos remotos.
- Se debe mantener monitoreada las redes de datos para garantizar su disponibilidad, rendimientos y seguridad, facilitando la gestión de incidentes y generar los reportes periódicos con el resultado de dicha monitorización.
- Se deben contar con respaldos de las configuraciones, y un plan de recuperación documentado y probado, que permita corroborar la integridad de estas.
- Cualquier conexión con redes externas debe ser debidamente autorizada por la jefatura correspondiente y cuenta con medidas de seguridad para evitar incidentes o accesos no autorizados.
- Se encuentran prohibidas las conexiones de dispositivos que no cumplan con las medidas de seguridad definidas.
- Los sistemas y dispositivos de comunicaciones conectados a la red deben estar correctamente configurados para evitar la posibilidad de que se pueda explotar vulnerabilidades, que puedan afectar la seguridad y rendimiento de la red.
- Se debe gestionar con proveedores los procedimientos técnicos, de operación y mantenimiento de la red.
- Se debe realizar análisis de vulnerabilidades y pruebas de intrusión controlados en la infraestructura de redes.
- Los dispositivos de comunicación deben contar con el firmware estable del fabricante.
- Se debe proteger con cortafuegos y sistemas de prevención de intrusos todas las interfaces existentes entre las redes internas y las redes externas.

5.5. Sobre la segregación en las redes

- La red debe estar segmentada y contemplando aspectos como aislamiento, a nivel lógico, de entornos de producción, desarrollo, redes usuarias, servidores, zonas desmilitarizadas (DMZ) a nivel de firewall.
- Las redes de invitados no deben tener conexión con redes las redes internas.

5.6. Dominios de seguridad.

- Se deben identificar los dominios de seguridad requeridos en la arquitectura de la institución. Estos dominios deben ser definidos de acuerdo con el nivel de confianza y de los recursos críticos que contengan.
- Se debe establecer una clasificación estándar de los niveles de confianza asociables a los dominios de seguridad identificados como "Confiables", "Semi confiables" y "No Confiables".
- Las conexiones determinadas No Confiables deben ser protegidas y controladas por un Firewall.
- Se deben establecer los mecanismos de control de acceso que permitan implantar los flujos y sentidos de conexión autorizados entre los dominios definidos.
- No se debe permitir el acceso directo desde un dominio "No confiable" hacia el ambiente de Producción. Cualquier excepción debe ser evaluada y autorizada por el Encargado/a de Seguridad de la Información y Ciberseguridad.

5.7. De las actividades sobre la red y los sistemas computacionales

- Los usuarios no accederán a los sistemas de información del MINVU sin contar con las autorizaciones necesarias para ello.
- Los usuarios no utilizarán herramientas, orientadas a atacar, vulnerar o alterar los sistemas de información.
- Los usuarios no instalarán ningún tipo de hardware o software por iniciativa propia, sin la autorización del jefe de la División Informática o jefe del Departamento de Soporte Tecnológico de la División de Informática.
- Los usuarios no ejecutarán programas que exploten alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el administrador.
- Se prohíbe cargar, almacenar, publicar, difundir, distribuir o transmitir, por medio de los recursos informáticos de la Institución, archivos, programas, música, video, que violen las leyes sobre la propiedad intelectual.
- Se prohíbe cargar, almacenar, publicar, difundir, distribuir o transmitir, por medio de los recursos informáticos de la Institución, de forma intencional, archivos que contengan virus o datos falsos.
- Se prohíbe abusar de brechas de seguridad o generar interrupciones en el funcionamiento de las redes de comunicaciones. Las brechas de seguridad incluyen, pero no se limitan a, acceder datos de los cuales no es un receptor autorizado, o conectarse a un servidor al cual no ha sido expresamente autorizado, salvo que sean tareas dentro del contexto de labores habituales. Para efectos de esta sección, se entiende, pero no se limita a, interrupciones como: falsificación de paquetes de comunicación, denegaciones de servicio, entre otras.
- Se prohíbe realizar chequeos de seguridad, a menos que se notifique al jefe de la División de Informática del MINVU y éste apruebe la actividad.
- Se prohíbe ejecutar cualquier clase de monitoreo de redes que implique interceptar datos desde los computadores de los funcionarios, salvo que dicha actividad sea parte del trabajo habitual del funcionario.
- Se prohíbe usar programas para enviar mensajes de cualquier tipo, con la intención de interferir o deshabilitar la conexión de un usuario de la red computacional.
- Se prohíbe entregar información de la institución, como base de datos, listados de funcionarios y/o cualquier otra información sensible a personas o instituciones fuera de MINVU.

5.8. Registro de eventos.

- Se debe implementar las reglas o configuraciones de los registros de todos los eventos importantes relativos al acceso a las redes y a los servicios a las redes.
- Se debe implementar las reglas o los medios de protección de los registros de eventos contra su alteración y acceso no autorizado.

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

N° Versión	Fecha Aprobación	Motivo de la revisión
01	Diciembre 2012	Versión inicial.
02	Diciembre 2013	Incorporación de definiciones institucionales
03	Noviembre 2017	Se actualizan "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/ Jefe 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; Claudia Ernst Valencia/ Jefe División Administrativa.

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

MMV/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