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°14.493, (V. Y U.), DE 2017, RESOLUCIÓN EXENTA N° 14.478, (V. Y U.), DE 2017 Y RESOLUCIÓN EXENTA N°14.483, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE CUENTAS DE USUARIO Y USO DE LAS CONTRASEÑAS, 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° 3094 /

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 Cuentas de Usuario aprobada por Resolución Exenta 14.493, (V. y U.), de 2017, la Política Específica de Seguridad de Uso de las Contraseñas aprobada por Resolución Exenta 14.478, (V. y U.), de 2017 y la Política específica de identificación y autenticación aprobada por Resolución Exenta 14.483, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

I. **Derógase** la Política Específica de Seguridad de Cuentas de Usuario aprobada por Resolución Exenta 14.493, (V. y U.), de 2017.
II. **Derógase** la Política Específica de Seguridad de Uso de las Contraseñas aprobada por Resolución Exenta 14.478, (V. y U.), de 2017.
III. **Derógase** la Política específica de identificación y autenticación aprobada por Resolución Exenta 14.483, (V. y U.), de 2017.
IV. **Apruébese** la Política Específica De Seguridad De Cuentas De Usuario y Uso De Las Contraseñas, la que se detalla a continuación:

"POLÍTICA ESPECÍFICA DE SEGURIDAD DE CUENTAS DE USUARIO Y USO DE LAS CONTRASEÑAS"

1. OBJETIVO

Esta política define las reglas que controlan la creación y mantención de cuentas de acceso a los sistemas computacionales y definir el uso y las prohibiciones de las contraseñas en el MINVU, considerando que la plataforma tecnológica institucional consolida todos los accesos en una única cuenta y contraseña por usuario.

2. ALCANCE

La presente Política, considerada como parte del Dominio de Control de Acceso, se 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 manifieste tal voluntad.

Esta política está relacionada con el cumplimiento del control A.09.04.03 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 control de acceso lógico.
- Normativa de gestión de control de acceso.

4. ROLES Y RESPONSABILIDADES

Jefe/a de División Informática

- Validar y autorizar las acciones necesarias para gestión de las cuentas de usuario y las contraseñas

Sección de Ingeniería y Explotación de Sistemas- División de Informática

- Disponer herramientas de seguridad para la gestión de cuentas de usuarios y las contraseñas.

Encargado/a de Seguridad de la Información y Ciberseguridad

- Velar por el cumplimiento de la presente política específica en la institución

Usuarios

- Cumplir con las definiciones establecidas en esta política.

5. REGLAS DE LA POLÍTICA

5.1 Acerca de las Cuentas de Usuario

5.1.1 Generalidades de las Cuentas de Usuario

- Todo usuario que requiera tener acceso a cualquier recurso computacional, debe contar con un mecanismo que lo identifique (cuenta de usuario) y lo autentifique mediante una contraseña o dispositivo de autenticación, en forma positiva.
- El mecanismo de autenticación (contraseñas, dispositivo u otro) debe ser asignados individualmente, siendo de uso exclusivo para el usuario designado.
- En el nivel de cuentas de usuario, se definen niveles de accesos y privilegios a las distintas aplicaciones de la Institución. Su función es establecer perfiles propios para cada cargo funcional, los que serán usados como perfil por omisión si no se especifican otras características.
- A nivel de cuentas de Administrador, se definen los accesos y privilegios solo a personal técnico calificado y que cumplen las funciones de soporte y administración de sistemas operativos y dispositivos componentes de la red.

5.1.2 Individualidad de las cuentas de usuario

- La cuenta de usuario y la clave, asociados a una cuenta de usuario, son individuales, estando prohibido facilitarlos a un tercero.
- El usuario dueño de la cuenta es responsable de las actividades que se efectúen con su cuenta de usuario, pudiendo recibir sanciones disciplinarias por sus actos.
- Estas disposiciones rigen para usuarios finales internos o externos, operadores, administradores y auditores.

5.1.3 Creación de cuentas de usuario

- Los usuarios deben identificarse en su computador y en la red interna con un Identificador de Cuenta Único, también conocido como Username o cuenta de usuario.
- Toda nueva cuenta de usuario que se cree debe ser definida por el Grupo de Operaciones, a modo de garantizar su unicidad.
- La creación de una nueva cuenta de usuario debe regirse de acuerdo con el Procedimiento de Creación de Cuentas de Usuario correspondiente.
- El Grupo de Operaciones de la Sección de Ingeniería y Explotación de Sistemas debe velar por el almacenamiento y actualización de la información asociada a la cuenta creada.
- La nomenclatura usada para la composición del Cuenta de usuario que identifica cada cuenta debe cumplir con un estándar de nomenclatura de Cuentas de Usuario.
- Cualquier solicitud de cambio de privilegios asignados a una cuenta debe ser hecha por el Jefe del Área de su dependencia directa y validada por el Propietario del proceso de negocio.
- En caso de desvinculación se deberá aplicar Procedimiento para la baja o desvinculación de usuarios correspondiente. En caso de cambio de área el Jefe de área de su dependencia directa deberá informar al Encargado de Sección de Ingeniería y Explotación de Sistemas de la División de informática.

5.1.4 Usuario Anónimo y Cuentas genéricas

- No se deben usar conexiones anónimas o cuentas con nombres genéricos para acceder a ningún sistema interno. La jefatura de la División de Informática puede autorizar excepciones a esta norma, siempre y cuando este acceso sea debidamente controlado (trazable), seguro y por un periodo de tiempo limitado.

5.1.5 Cuentas de usuarios externos

- La solicitud de cuenta y clave para usuarios externos al MINVU, debe ser formal y puede solicitarla solamente el contacto administrativo definido en el contrato con la empresa externa. La solicitud debe ser autorizada por la jefatura de la División Informática.
- Para la creación de cuentas de usuarios externos, se debe indicar el motivo del requerimiento, y la fecha de expiración.
- El Grupo de Operaciones de la Sección de Ingeniería y Explotación de Sistemas debe revisar periódicamente que las cuentas de usuarios externos expiradas sean borradas o cerradas.
-

5.1.6 Manejo de Cuentas de Administración

- Se deben crear cuentas personalizadas para los administradores, con los privilegios pertinentes y claves robustas. No se deben usar cuentas estándares de administración de los sistemas.
- Las cuentas de administración que se puedan borrar, sin generar incidente de seguridad por funcionalidad del sistema, deben ser borradas. Aquellas cuentas que no se puedan borrar, se les debe asignar una clave robusta, la que será guardada bajo protocolo seguro.
- El Encargado de Seguridad de la Información, a través del Jefe de División informática de la Subsecretaría, debe revisar, periódicamente, la seguridad en la custodia de estas claves.
- No se permite la asignación de privilegios de administración a cuentas que no pertenezcan al grupo de administradores. Cualquier excepción debe ser autorizada formalmente, por un período fijo, por la jefatura de la División Informática. Esta autorización temporal debe ser controlada por Encargado de Sección de Ingeniería y Explotación de Sistemas.

5.1.7 Monitoreo y auditoría de cuentas de usuario

- Se deben monitorear las actividades efectuadas por cuentas con privilegios, las que requieren ser individualizadas.
- Periódicamente, se deben auditar las cuentas existentes, para chequear que sólo se encuentren aquellas debidamente autorizadas. Esta revisión cobra vital importancia, con las cuentas de usuarios con altos privilegios (cuentas de administración).

5.2 Acerca del uso de las contraseñas.

5.2.1 Generalidades del uso de las contraseñas

- Las contraseñas son de carácter personal e intransferible, al igual que las cuentas de usuario, no permitiéndose que otras personas hagan uso de ella; de esa manera, cada usuario que disponga de una cuenta de usuario será el único responsable de las acciones efectuadas bajo el uso de su cuenta personal.
- Todo usuario de cualquier sistema computacional debe tener una cuenta de usuario única, con un perfil de acceso de acuerdo con su función o derechos, y con una contraseña inicial que debe ser cambiada sólo por él.
- Todas las contraseñas deben cumplir con varias características de seguridad definidas y fijadas por la División de Informática de la Subsecretaría.
- Si un usuario considera que su cuenta o contraseña ha sido comprometida o revelada sin su autorización, deberá declararlo como un incidente de seguridad para que se investigue si ha sufrido algún daño, y proceda a cambiar sus credenciales.
- El largo de las contraseñas de los usuarios lo establece la División de informática de la Subsecretaría.
- El largo y configuración de la contraseña debe ser verificado, en forma automática, al momento de crearla o modificarla.
- El uso de contraseña igual a la cuenta de usuario o en blanco no se encuentra permitido.
- Las contraseñas creadas por el usuario deben ser difíciles de adivinar por terceros y ser sólo de su conocimiento personal, quedando prohibido su divulgación, así como mantener anotada su contraseña en lugar visible.
- Las cuentas de servicios y procesos automáticos deben ser tratadas con las mismas restricciones establecidas para las cuentas de usuario; respecto de no utilizar múltiples accesos para una misma cuenta.
- En los sistemas aplicativos, no está permitido el uso de contraseñas "en duro".

5.2.2 Cambio periódico de las contraseñas

- La contraseña inicial asignada a una cuenta nueva de usuario debe crearse expirada, de modo de obligar su cambio en su primer acceso.
- Todos los usuarios deben cambiar su contraseña en forma periódica
- Las contraseñas de los usuarios deben contar con un archivo histórico, debidamente encriptado, con el objetivo de no permitir reutilizar una contraseña próxima utilizada.

5.3 Uso prohibido

- Mantener las contraseñas de forma tal que pueda ser fácilmente divulgada o conocida por terceros.
- Divulgar la contraseña personal o de terceros a otras personas.
- Ejercer cualquier tipo de acción tendiente a conocer o adivinar una contraseña de una cuenta para la que no se tiene autorización expresa.

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
01	Diciembre 2012	Versión inicial
02	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.
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/ 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, de 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

MINISTERIO DE VIVIENDA Y URBANISMO

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

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

MMV/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