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° 14.475, (V. Y U.), DE 2017, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD DE CONTROL DE CAMBIOS, 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° 3095 /

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 Control de Cambios, aprobada por Resolución Exenta 14.475, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

I. **Derógase** la Política Específica de Control de Cambios aprobada por Resolución Exenta 14.475, (V. y U.), de 2017.

II. **Apruébese** la Política Específica de Seguridad de Control de Cambios, la que se detalla a continuación:

"POLÍTICA ESPECÍFICA DE SEGURIDAD DE CONTROL DE CAMBIOS"

1. OBJETIVO

Esta política establece las reglas que regula el proceso de cambio en la infraestructura computacional del MINVU.

2. ALCANCE

La presente Política, considerada como parte del Dominio de Seguridad de las Operaciones, Adquisición, Desarrollo y Mantenimiento de Sistemas 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 de los controles A.12.01.02, A.14.02.02 y A.14.02.03 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 cambios.

4. ROLES Y RESPONSABILIDADES

Encargado de Sección de Ingeniería y Explotación de Sistemas - División de Informática

- Planificar, coordinar y/o ejecutar los cambios en la plataforma del ambiente de Producción (dispositivos, servidores, sistema operativo, software básico).
- Planificar e instalar los nuevos Sistemas Aplicativos o actualizaciones en los ya existentes.
- Controlar que existan las aprobaciones del Usuario y Área QA antes de realizar los cambios solicitados.
- Planificar y ejecutar los cambios en el hardware y software básico.

Encargado de Mesa de Atención de Usuarios- División de Informática

- Coordinar los cambios que se producen en los ambientes de Test y Producción, para el traspaso de Sistemas Aplicativos.
- Atender las peticiones y requerimientos de los usuarios de la Institución, ante incidentes y cambios mayores en los Sistemas Aplicativos que son implantados e Producción.

Jefaturas de Sección Sistemas de Apoyo al Negocio y Sección Plataforma Tecnológica de Subsidios- División de Informática

- Documentar las modificaciones de los Sistemas Aplicativos afectados por un cambio mayor, a nivel de usuario, para establecer las necesidades y documentos de capacitación necesarios, con el objetivo de difundir los cambios y apoyar la implantación de los nuevos procesos. Realizar la revisión de calidad del software aplicativo nuevo o existente.
- Aprobar o rechazar los cambios del software aplicativo nuevo o existente antes de su paso a producción.

Encargado de Sección de Gestión de Proyectos y Calidad - División de Informática

- Realizar la revisión de calidad del software aplicativo nuevo o existente.
- Aprobar o rechazar los cambios del software aplicativo nuevo o existente antes de su paso a producción.

Jefe División Informática y Jefes de Departamento y Sección- División de

Informática

- Aprobar y Autorizar excepciones para cambios en producción sin aprobación del Área de Control de Calidad (QA).
- Autorizar cambios que afecten la disponibilidad de los sistemas.

Jefe de Proyecto – División Informática

- Solicitar los cambios en producción del software aplicativo nuevo o existente, incluyendo las aprobaciones del usuario y área QAS o la excepción del Jefe de Departamento o Jefe DINFO.
- Certificar que los cambios fueron correctamente aplicados.

Encargado/a de Seguridad de la Información y Ciberseguridad

- Velar por el cumplimiento de esta política.

5. REGLAS DE LA POLÍTICA

5.1 Consideraciones generales

Cualquier cambio de hardware, software básico y Sistemas Aplicativos que se requiera efectuar en el ambiente de Producción, necesariamente debe considerar los siguientes aspectos, que se deben cumplir antes del proceso de cambio:

- Desarrollar una planificación detallada de cada una de las etapas, incluyendo la definición de respaldos previos, recursos necesarios para el proceso del cambio, conjunto de pruebas pre y post-instalación, capacitación de usuarios, criterios de éxito o aceptación, así como también un plan de vuelta atrás.

- Coordinar el cambio con las áreas involucradas o propietarios de los sistemas afectados, para que se efectúe durante períodos de baja carga de trabajo.

- Solicitar la correspondiente autorización a las jefaturas involucradas.

- Durante el proceso de cambio se debe contar siempre con la colaboración o contacto directo con los fabricantes del software o empresas de soporte relacionadas para garantizar la compatibilidad con versiones y actualizaciones futuras y tener toda la documentación actualizada. Además del original, los cambios realizados y las actualizaciones siguientes del software deberán guardarse por si es necesario reinstalar el software en el futuro.

- Mantener habilitado el máximo de detalle en la función de registro de auditoria relacionado con el cambio.

- Posterior al cambio efectuado, se requiere necesariamente registrar el cambio en los sistemas de control correspondientes.

5.2 Cambios de Hardware

La Sección de ingeniería debe planificar y solicitar al Área de Redes y Sistemas y/o a una tercera parte, los cambios al hardware que se requieran por mejoras o reparaciones ante fallas.
En el caso de participación de terceras partes, ellas deben ser controladas por el Área de Redes y Sistemas.

5.3 Cambios de Software básico

Los cambios producidos a nivel de software básico, deben cumplir son los siguientes requisitos:

- Los cambios deben ser programados de preferencia para los fines de semana o días no hábiles o fuera del horario de oficina.

- Cuando se realicen cambios en los sistemas operativos y software de base, se revisarán los sistemas y aplicaciones críticas para el negocio con el fin de asegurar que el cambio no ha tenido un impacto negativo en los mismos.
- No se debe instalar actualización sin verificar su autenticidad, integridad y evaluación de posible impacto a los sistemas aplicativos.

- Una etapa previa posible de considerar, es la instalación de la actualización en un ambiente aislado de prueba, con el objeto de realizar un chequeo de funcionamiento.

5.4 Cambios en los Sistemas Aplicativos

Los cambios a los Sistemas Aplicativos existentes y/o nuevos sistemas, deben considerar los siguientes aspectos:

- Ser analizado y probado previamente en los ambientes de Desarrollo y Test.

- Los datos de prueba deben ser concordantes con lo que se contiene en ambiente de Producción. Estos deben ser preservados para permitir pruebas repetitivas, en lo posible los datos para prueba y desarrollo deben corresponder a un subconjunto representativo de información de producción.

- Para los sistemas nuevos y de función crítica, deben realizarse pruebas tales como volumen, stress, rendimiento, almacenamiento, integración de sistemas, seguridad y recuperación ante errores.

- Contar con la aprobación del usuario líder.

- Generar la documentación necesaria definida para hacer entrega del cambio a Producción.

- Documentar detalladamente los cambios introducidos al sistema, de manera de facilitar la capacitación de los usuarios. Esta capacitación debe realizarse tan cerca de la salida a Producción como sea posible, de tal manera de disminuir el olvido de los usuarios.

- Si el Sistema Aplicativo es un desarrollo externo, se debe contar con el apoyo de personal de la empresa proveedora del sistema.

5.5 Cambios mayores en Sistemas Aplicativos

Los cambios mayores a los Sistemas Aplicativos existentes o nuevos sistemas, que afecten a la Institución de manera transversal, deben considerar:

- La incorporación de un equipo de personas al proyecto, con el propósito de registrar y documentar las diferencias a nivel de perfiles, datos, programas, interfaces usuarias para el sistema antiguo y nuevo.

- Planificar y ejecutar la capacitación del personal impactado.

- Apoyar la salida a Producción del sistema, incorporándose a la Mesa de Ayuda o constituyendo una mesa de ayuda especial.

5.6 Cambios de Emergencia

Se debe establecer un proceso definido y controlado para los cambios de emergencia. Este proceso debe considerar el registro post modificación de la información asociada y su correspondiente aprobación.

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	Noviembre 2011	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 "Actualización de contenidos generales
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 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 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

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