Ministerio de Vivienda y Urbanismo

Gobierno de Chile

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°14.492 (V. Y U.), DE 2017, Y APRUEBA POLÍTICA ESPECÍFICA DE SEGURIDAD PARA EL DESARROLLO DE SISTEMAS, EN EL MARCO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO.

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA
30 DIC 2019
RESOLUCION EXENTA
TRAMITADA

SANTIAGO, 30 DIC 2019

RESOLUCIÓN EXENTA N° 3073 /

VISTOS:

HOY SE RESOLVIO LO QUE SIGUE

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 Desarrollo de Sistemas aprobada por Resolución Exenta 14.492, (V. y U.), de 2017, dicto la siguiente:

RESOLUCIÓN:

I. **Derogase** la Política Específica de Seguridad de Desarrollo de Sistemas, aprobada por Resolución Exenta 14.492, (V. y U.), de 2017.

II. **Apruébese** la Política Específica De Seguridad Para El Desarrollo De Sistemas, la que se detalla a continuación:

"POLÍTICA ESPECÍFICA DE SEGURIDAD PARA EL DESARROLLO DE SISTEMAS"

1. OBJETIVO

Esta política define las reglas para el Desarrollo y Mantenimiento de Sistemas de información en el MINVU, estableciendo los criterios de seguridad que deben ser considerados desde las primeras etapas del desarrollo de sistemas, en particular en sus fases de planificación y diseño.

2. ALCANCE

La presente Política, considerada como parte del Dominio de Adquisición, Desarrollo y Mantenimiento de Sistemas, y 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 cual se manifieste tal voluntad.

Esta política está relacionada con el cumplimiento del control A.14.02.01 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 Uso De Controles Criptográficos.
- Política Específica De Seguridad De Uso Del Software.
- Normativa de Gestión de Desarrollo y Mantenimiento de Sistemas

4. ROLES Y RESPONSABILIDADES

Jefe de División Informática

- Validar y aprobar la Metodología de Desarrollo y Mantención de Sistemas que incorpore los requerimientos de seguridad a utilizar en el Ministerio.
- Gestionar la incorporación a la metodología de desarrollo del MINVU, de todas aquellas acciones que mitiguen las debilidades que se vayan publicando y conociendo, en el ámbito de la construcción y mantención de los sistemas de información.
- Apoyar la difusión y cumplimiento de esta política.
- Gestionar los recursos necesarios para la implementación de los ambientes de Desarrollo, Pruebas y Producción.

Encargado de Sección Ingeniería y Explotación de Sistemas

- Disponer de medidas de protección adecuadas para el desarrollo y mantenimiento correcto y seguro de los sistemas de información.

Encargados de Sección para el Desarrollo de Sistemas

- Acordar con el Encargado de Seguridad Informática de la División de Informática la configuración de seguridad estándar.
- Cumplir con las disposiciones definidas en esta política.
- Documentar el Sistema y/o sus modificaciones.

Departamento de Soporte Tecnológico a la Gestión

- Recibir, canalizar y gestionar cualquier aviso de problema o incidente en la operación de los sistemas de información.

Encargado de Seguridad Informática de la División de Informática

- Coordinar revisiones periódicas de seguridad en los sistemas de producción.
- Proponer buenas prácticas de seguridad para el desarrollo de sistemas.

Encargado/a de Seguridad de la Información y Ciberseguridad

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

5. REGLAS DE LA POLÍTICA

5.1. Consideraciones Generales

- Los Departamentos de desarrollo de sistemas son responsables de planificar y ejecutar el mantenimiento de los sistemas de la Institución. Además, deben planificar y coordinar con el área de calidad del software (QA) la ejecución de pruebas de funcionamiento de los sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción.

- Se debe estandarizar el ciclo de desarrollo de sistemas, tal como lo establece la Metodología desarrollo y mantención de sistemas definidos en el MINVU.

- Se deben establecer estándares de criterios de seguridad y de calidad en el desarrollo de sistemas.

- Toda modificación de software crítico por parches o módulos adicionales, debe ser analizada previamente en los ambientes de desarrollo y prueba.

- Se deben planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y post-instalación, criterio de aceptación del cambio y un plan de vuelta atrás.

- Los programadores y personal de terceros no deben tener acceso a información de producción que contengan información sensible.

- Para propósitos de desarrollo y pruebas, los responsables deben generar sus propios datos, debiendo ser éstos distintos a los que se encuentran en ambiente de producción.

- El sistema desarrollado o modificado por terceras partes, debe cumplir con lo establecido en esta política, incluyendo los criterios de seguridad establecidos en ella.

5.2. Desarrollo realizado por Terceros

- Se debe establecer un acuerdo previo con empresas de desarrollo externas que resguarden la propiedad intelectual, y aseguren los niveles de confidencialidad de la información manejada en el proyecto.

- Se debe diferenciar entre el encargado de establecer y autorizar los acuerdos con terceros, de los que deban auditar su cumplimiento.

5.3. Gestión de Vulnerabilidades

- Se debe establecer una gestión de vulnerabilidades técnicas, orientada a analizar los vacíos de seguridad (vulnerabilidades) que surgen en los productos de software por fallas de seguridad que son publicadas en Internet por los proveedores de tecnología asociada y proponer las medidas de mitigación al riesgo definido.

- Se deben efectuar validaciones y evaluaciones periódicas de seguridad durante el ciclo de vida del proyecto.

5.4. Documentación

- El diccionario de datos o repositorio debe mantener una descripción actualizada de las definiciones de datos.
- Si el programador incluye comentarios en el código fuente, éstos deben ser útiles para un tercero y no divulgar información de configuración innecesaria.

- Respecto a la documentación, se debe:
  - Generar durante el ciclo de desarrollo y no postergarla hasta el final.
  - Revisar por los usuarios finales del sistema bajo desarrollo.
  - Actualizar si el programa cambia alguna de sus funcionalidades.
  - Almacenar en un sitio centralizado (Servidor) de la División de Informática.

5.5. Evaluación o Casos de Negocio

- Como parte de esta fase se debe clarificar la problemática actual referida a la seguridad de la información, que debe ser cubierta por el nuevo sistema.

- En el estudio de factibilidad o anteproyecto, se debe considerar el aspecto de seguridad, en cuanto al nivel de criticidad del sistema y de los controles que se debieran predefinir.

5.6. Especificación detallada de Requerimientos

- En el análisis de factibilidad de los requerimientos, se debe considerar el nivel de criticidad del sistema, además del nivel de protección de seguridad que requerirán los datos y las aplicaciones que lo compongan.

- Los requerimientos de seguridad deben ser compatibles con lo que se establece en las otras Políticas de Seguridad.

5.7. Diseño del Sistema

- El nivel de sensibilidad debe ser definido para cada elemento de datos, archivo, programa y sistema.
- Si se define utilizar cifrado de datos, deben ser los definidos en el estándar de cifrados.
- Si se utiliza un administrador de bases de datos, se deben emplear las herramientas de seguridad que el producto provee.
- Todos los programas críticos deben incluir la generación de registros de auditoría, incluyendo como mínimo, la identidad del usuario que lee o escribe y la fecha/hora del evento. Estos registros deben ser protegidos contra la manipulación no-autorizada.

5.8. Codificación y Pruebas

- No está permitido modificar programas sin que quede registrado o documentado el cambio.
- Se deben usar las técnicas de programación modular, usando lenguajes de alto nivel.
- No está permitido escribir o modificar código auto-copiante o cualquier otro tipo de código malicioso (virus y gusanos), así como funciones u operaciones no documentadas o no autorizadas en los programas.
- En lo posible las pruebas del sistema deberían incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores.
- En lo posible, las pruebas deben ser realizadas en forma automática, almacenando criterios y datos de pruebas en archivos, de modo de permitir la verificación rápida y repetitiva.

5.9. Implementación

- Se debe velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.
- Se debe efectuar la sintonía o ajuste (tuning) de los controles establecidos en la fase de diseño.

5.10. Post Implementación

- Se deben revisar y auditar la existencia de los controles de seguridad, definidos en la etapa de diseño.

5.11. Controles a implementar

- Se deben considerar e implementar, al menos los siguientes controles:
  - Validación de datos de entrada y de salida.
  - Controles de procesamiento interno.
  - Controles criptográficos.
  - Protección de los datos de prueba.
  - Segregación de Acceso a Datos.

6. DIFUSIÓN

La comunicación y difusión de la presente política específica es responsabilidad de cada Encargado/a de Seguridad de la Información o 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 Aprobación	Motivo de la revisión
01	Diciembre 2012	- Versión inicial
02	Noviembre 2017	- Se actualizan "Considerando" y "Objetivo"
03	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 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

GUILLERMO ROLANDO VICENTE
SUBSECRETARIO DE VIVIENDA Y URBANISMO

MMV/MAG/AGG/CPP/LCC

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

PABLO ZAMBRANO TORQUERA
INGENIERO DE EJECUCION
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