2 DE FEBRERO DE 2021

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

SERVIU METROPOLITANO

A.05.01.01
POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

NORMA NCH-ISO 27001:2013

SERVIU
Region Metropolitana

Ministerio de Vivienda y Urbanismo

APRUEBA INTEGRACIÓN DE LA VERSIÓN N° 08 DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE VIVIENDA Y URBANISMO Y DEJA SIN EFECTO ANTERIORES VERSIONES RELACIONADAS CON ESTA MATERIA.

Departamento de Programación Física y Control
Sección Planificación
OFPA N° 16

CON ESTA FECHA SE HA DICTADO LA SIGUIENTE:

RESOLUCIÓN EXENTA Nº _____/

SANTIAGO, 4675 *27.09.2019

VISTOS:

a. Lo dispuesto en la Ley Nº 18.575 de 2001, Orgánica Constitucional de Bases Generales de la Administración del Estado, el Decreto Supremo Nº 355/1976 (V. y U.) Reglamento Orgánico de los Servicios de Vivienda y Urbanización; y el Decreto Ley Nº 1305, que restructura y regionaliza el Ministerio de la Vivienda y Urbanismo, de 1975;

b. Lo dispuesto en el Decreto Nº 83/2004 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;

c. Lo dispuesto en la Norma NCh-ISO 27001:2013 de Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información – Requisitos;

d. El Instructivo Presidencial Nº 008 de 2018, que imparte Instrucciones en materia de Ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los Órganos de la Administración del Estado;

e. La Resolución Exenta Nº 3249, de fecha 12 de julio de 2019, que actualiza y complementa la Estructura, Roles y Responsabilidades del Comité de Seguridad de la Información, en el SERVIU Metropolitano;

f. La Resolución Exenta Nº 2097, de fecha 12 de septiembre de 2019, del Ministerio de Vivienda y Urbanismo que aprueba la Política General de Seguridad de la Información del MINVU, versión 08, para ser implementada en las 16 Secretarías Regionales Ministeriales de Vivienda y Urbanismo, en los 16 Servicios de Vivienda y Urbanización, en el Parque Metropolitano de Santiago, y en la Subsecretaría de Vivienda y Urbanismo;

g. La Resolución Nº 7 y 8, de fecha 26/03/2019 y 27/03/2019, respectivamente, de la Contraloría General de la República, que Fija Normas sobre Exención del trámite de Toma de Razón, y que determina los montos en unidades tributarias mensuales, a partir de los cuales los actos que se individualizan quedarán sujetos a Toma de Razón o Controles de Reemplazo cuando corresponda;

h. El Decreto TRA Nº 272/46/2018 de (V. y U.) de fecha 18 de julio de 2018, que me nombra como Director titular del Servicio de Vivienda y Urbanización Metropolitano, y las facultades que en tal carácter me competen en conformidad al D.S. Nº 355 de (V. y U.) de 1976, Reglamento Orgánico de los Servicios de Vivienda y Urbanización; dicto lo siguiente;

CONSIDERANDO:

a. La revisión realizada por el Comité de Seguridad de la Información del SERVIU Metropolitano, que aprueba la integración de la Política de Seguridad de la Información.

b. La necesidad de integrar la Política General de Seguridad de la Información del MINVU, versión 08, para ser implementada en las 16 Secretarías Regionales Ministeriales de Vivienda y Urbanismo, en los 16 Servicios de Vivienda y Urbanización, en el Parque Metropolitano de Santiago, y en la Subsecretaría de Vivienda y Urbanismo, la que se detalla a continuación:

RESOLUCIÓN:

1. **APRUÉBASE** la Integración, aplicación y difusión en el SERVIU Metropolitano, de la Política General de Seguridad de la Información, del Ministerio de Vivienda y Urbanismo, en su Versión N° 08, a partir de la fecha de tramitación de la presente Resolución.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO:

- Proteger los activos físicos y digitales de SERVIU Metropolitano, basado en preservar los principios de confidencialidad, integridad y disponibilidad de la Información, identificando oportunamente los riesgos asociados a los productos Estratégicos (bienes y/o servicios), establecidos en las Definiciones Estrategias Institucionales (Formulario A1), asegurando la continuidad Operacional.

2. ALCANCE:

- Es aplicable al personal del Servicio cuya calidad jurídica es Planta, Contrata y Honorarios, así como también a las personas que cumplen funciones específicas en el Servicio, tal como Asesores, Consultores y Practicantes, es decir, a todas las personas que trabajan o colaboran en SERVIU Metropolitano, incluyendo a las empresas que prestan servicios en este organismo y que, para su desempeño, hacen uso y acceden a todo tipo de información y a los productos Estratégicos (bienes y/o servicios), establecidos en las Definiciones Estrategias Institucionales (Formulario A1).

3. ROLES Y RESPONSABILIDADES:

- Los roles y responsabilidades de las personas que componen el Comité de Seguridad de la Información, del SERVIU Metropolitano, son los siguientes:

Cargos Responsables	Roles Claves
- **Director(a) SERVIU Metropolitano.**	1. Designar a los responsables del proceso de Seguridad de la Información, en el Servicio; 2. Sancionar las Políticas y Estrategias diseñadas para gestionar la Seguridad de la Información en el Servicio.
- **Encargado(a) de Seguridad de la Información.** - Subdirector(a) de Administración y Finanzas	1. Aprobar toda la documentación que genera el Sistema de Seguridad de la Información, en el Servicio; 2. Supervisar y velar por el cumplimiento e implementación del proceso de Seguridad de la Información en SERVIU Metropolitano.
- **Coordinador(a) de Seguridad de la Información.** - Jefe(a) Departamento de Programación Física y Control	1. Presidir las reuniones del Comité de Seguridad de la Información; 2. Coordinar las reuniones periódicas que realice el Comité de Seguridad de la Información; 3. Validar las Actas y acuerdos que se generen, producto de las reuniones periódicas que efectúe el Comité de Seguridad de la Información; 4. Gestionar la aprobación de Políticas, con el Encargado(a) de Seguridad de la Información del Servicio; 5. Coordinar con el Encargado(a) PMG de Seguridad de la Información el cumplimiento de los controles comprometidos y sus respectivos verificadores.

Cargos Responsables	Roles Claves
- **Encargado(a) PMG Sistema Seguridad de la Información.** - Profesional Departamento de Programación Física y Control.	1. Revisar y difundir la Guía Metodológica enviada por la Red de Expertos del PMG del Sistema de Seguridad de la Información al Servicio; 2. Actualizar la documentación de los controles transversales comprometidos por el Ministerio de Vivienda y Urbanismo y que se integran al SERVIU Metropolitano; 3. Realizar y dirigir las reuniones con los Encargados(as) de Activos y Encargados(as) de Incidentes del Sistema de Seguridad de la Información; 4. Elaborar procedimientos y/o documentación para el cumplimiento de los controles del Sistema de Seguridad de la Información; 5. Informar al Comité de Seguridad de la Información, la documentación vigente y actualizada del proceso de Seguridad de la Información; 6. Reportar al Encargado(a) del PMG Institucional y al Encargado(a) de Seguridad de la Información, los controles comprometidos para su implementación en el Servicio; 7. Difundir a través de la Sección de Comunicaciones del Servicio, las Políticas y Procedimientos implementados, del Sistema de Seguridad de la Información; 8. Realizar el seguimiento mensual de todos los controles comprometidos, en el Sistema Seguridad de la Información; 9. Informar mensualmente al Coordinador(a) de Seguridad de la Información, el estado de todos los controles; 10. Registrar y resguardar los documentos "Actas y acuerdos" que se levanten, producto de las reuniones periódicas que efectúa el Comité de Seguridad de la Información; 11. Diseñar el Programa para la Charla o Taller de Inducción en Seguridad de la Información.
- **Encargado(a) PMG Institucional.** - Jefe(a) Sección Planificación y Control	1. Remitir información recibida de la Subsecretaría de Telecomunicaciones (SUBTEL) y de la Secretaria General de la Presidencia (SEGPRES) al Encargado(a) PMG de Seguridad de la Información; 2. Monitorear el reporte periódico entregado por el Encargado(a) de PMG de Seguridad de la Información, del avance de los controles comprometidos; 3. Revisar las Políticas y Procedimientos del Sistema de Seguridad de la Información; 4. Ingresar y validar ante los Organismos SEGPRES y SUBTEL, el avance logrado, de los controles comprometidos; 5. Ingresar a la Plataforma de la DIPRES, el resultado efectivo alcanzado en el periodo; 6. Participar en las reuniones del Comité de Seguridad de la Información; 7. Participar en las reuniones que realiza el Ministerio de Vivienda y Urbanismo, para tratar temas de Seguridad de la Información; 8. Informar al Ministerio de Vivienda Y Urbanismo, el avance logrado por el Servicio, de los controles comprometidos.

Cargos Responsables	Roles Claves
- **Encargado(a) Activos de Información Físicos.** - Jefe(a) Sección Partes y Archivos.	1. Participar en la elaboración de las Políticas y Procedimientos propios de la Sección Partes y Archivos; 2. Participa en la revisión de Políticas específicas y documentos relacionados al Sistema de Seguridad de la Información, de la Sección Partes y Archivos.
- **Encargado(a) Activos de Información Físicos.** - Ministro(a) de FE	1. Participar en la eliminación segura de los activos de Información Físicos; 2. Participar en las reuniones del Comité de Seguridad de la Información.
- **Encargado(a) Gestión de las Personas para la Seguridad de la Información.** - **Encargado(a) Infraestructura para la Seguridad de la Información.** - **Encargado(a) Reportes y Registros de Incidentes de Seguridad de la Información.** - Jefe(a) Departamento Administrativo. - Encargado(a) de Equipo de Prevención de Riesgos y Ambientes Laborales.	1. Participar en la elaboración de las Políticas y Procedimientos propios del Departamento Administrativo; 2. Participar de la revisión de Políticas específicas y de los documentos relacionados con el Sistema de Seguridad de la Información, del respectivo Departamento Administrativo. 3. Desarrollar, documentar y mantener las Políticas de Seguridad propias de su área y velar por su correcta aplicación en el SERVIU Metropolitano; 4. Gestionar la confección de Planes de Continuidad para actuar frente a contingencias; 5. Coordinar con las áreas correspondientes, las instancias necesarias para activar los Planes de Continuidad en el Servicio; 6. Realizar las gestiones con las áreas correspondientes, que permitan recuperar las operaciones normales del Servicio; 7. Planificar, gestionar y evaluar pruebas, simulacros y ejercicios de contingencia; 8. Reportar, registrar, solucionar y escalar Incidentes de Seguridad de la Información, informando al Encargado(a) de Seguridad de la Información y al Encargado(a) del PMG de Seguridad de la Información.
- **Encargado(a) Activos de Información Digitales.** - **Encargado(a) Infraestructura para la Seguridad de la Información.** - **Encargado(a) Reportes y Registros de Incidentes de Seguridad de la Información.** - Jefe(a) Sección Informática.	1. Participar en la elaboración de las Políticas y Procedimientos propios de la Sección de Informática. 2. Desarrollar, documentar y mantener las Políticas de Seguridad de la Información, en el ámbito Informático, velando por su correcta aplicación en el SERVIU Metropolitano; 3. Liderar las soluciones otorgadas a los Incidentes de Seguridad de la Informática; 4. Participar en las reuniones de Comité de Seguridad de la Información; 5. Validar y proponer al Encargado (a) PMG de Seguridad de la Información, los planes de contingencia para asegurar la Continuidad de Operaciones Informáticas críticas de la Institución; 6. Controlar e investigar Incidentes y/o violaciones de Seguridad Informática e informar oportunamente a las Jefaturas del Servicio y al Encargado(a) PMG de Seguridad de la Información, de la situación detectada; 7. Reportar, registrar, solucionar y escalar Eventos e Incidentes de Seguridad de la Información, informando de ello al Encargado(a) de Seguridad de la Información y al Encargado(a) PMG de Seguridad de la Información.

Cargos Responsables	Roles Claves
- **Encargado(a) Infraestructura para la Seguridad de la Información.** - **Encargado(a) Reportes y Registros de Incidentes de Seguridad de la Información.** - Jefe(a) Departamento Servicios Generales.	1. Participar en la elaboración de las Políticas y Procedimientos propios del Departamento de Servicios Generales, del Servicio; 2. Desarrollar, documentar y mantener las Políticas de Seguridad propias de su área y velar por su correcta aplicación en el SERVIU Metropolitano; 3. Validar y proponer al Encargado (a) PMG de Seguridad de la Información, los planes de contingencia para asegurar la Continuidad de Operaciones críticas de la Institución; 4. Reportar, registrar, solucionar y escalar Eventos e Incidentes de Seguridad de la Información, informando de ello al Encargado(a) de Seguridad de la Información y al Encargado(a) PMG de Seguridad de la Información. 5. Realizar las gestiones con las áreas correspondientes que permitan recuperar las operaciones normales del Servicio; 6. Comunicar y difundir los alcances correspondientes, sobre la Política de Seguridad de Información para las Relaciones con el Proveedor.

4. DEFINICIONES:

- El SERVIU Metropolitano reconoce el valor de la información como un activo fundamental de la organización que necesita ser debidamente protegido, minimizando los riesgos y asegurando la continuidad operacional de sus funciones, tomando en cuenta los tres aspectos fundamentales en la Seguridad de la Información, la confidencialidad, integridad y disponibilidad de sus activos de información.

- Esta Política, tiene como objetivo gestionar la Seguridad de la Información dentro del Servicio y mantener la continuidad operacional de los activos de Información, de acuerdo a los controles comprometido a implementar durante el año t, que son necesarios para garantizar que, tanto los activos físicos y digitales, sean accesibles para el personal del Servicio y las personas que cumplen funciones específicas en la Institución, revisando periódicamente el cumplimiento de la implementación de los controles, a través de prácticas de seguridad y mecanismos que aseguren la integridad de los activos de Información contenida en equipos, sistemas e infraestructura.

- Establecer los controles a implementar durante el año t en el SERVIU Metropolitano:

Controles de Seguridad de la Información	
Control	**Objetivo del Control**
A.05.01.01	Políticas para la Seguridad de la Información.
A.05.01.02	Revisión de las Políticas de Seguridad de la Información.
A.06.01.01	Roles y responsabilidades de la Seguridad de la Información.
A.06.01.02	Segregación de funciones.
A.06.01.03	Contacto con autoridades.
A.06.02.01	Política de dispositivos móviles.
A.07.01.01	Selección.

A.07.02.01	Responsabilidades de la dirección.
A.07.02.02	Concientización, educación y formación en seguridad de la información.
A.07.02.03	Proceso disciplinario.
A.07.03.01	Responsabilidades en la desvinculación o cambio de empleo.
A.08.01.01	Inventario de activos.
A.08.01.04	Devolución de activos
A.08.03.01	Gestión de los medios Removibles.
A.08.03.02	Eliminación de los medios.
A.08.03.03	Transferencia física de los medios.
A.09.01.01	Política de control de acceso.
A.09.01.02	Acceso a las redes y a los servicios de la red.
A.11.01.01	Perímetro de seguridad física
A.11.02.01	Ubicación y protección del equipamiento.
A.11.02.04	Mantenimiento del equipamiento.
A.11.02.07	Seguridad en la reutilización o descarte de equipos.
A.11.02.08	Equipo del usuario desatendido.
A.11.02.09	Política de escritorio y pantalla Límpios.
A.12.02.01	Controles contra código malicioso.
A.12.03.01	Respaldo de la Información
A.12.04.01	Registro de eventos
A.12.06.02	Restricciones sobre la instalación de software.
A.15.01.01	Política de seguridad de la información para las relaciones con el proveedor.
A.15.02.01	Supervisión y revisión de los servicios del proveedor
A.16.01.01	Responsabilidades y Procedimientos.
A.16.01.02	Informe de Eventos de Seguridad de la Información.
A.16.01.05	Respuesta ante Incidentes de Seguridad de la Información.
A.17.01.01	Planificación de la continuidad de la seguridad de la información
A.18.01.03	Protección de los Registros
A.18.01.04	Privacidad y Protección de la Información de Identificación personal.
A.18.02.01	Revisión Independiente de la Seguridad de la Información

5. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN:

- La evaluación y revisión de la Política General de Seguridad de la Información, deberá efectuarse, al menos, una vez al año por el Comité de Seguridad de la Información (CSI), o a solicitud de la Jefatura superior del Servicio. Asimismo, frente a un cambio de contexto de la Institución, deberá asegurar su continuidad, idoneidad y confiabilidad al respecto.
- La formalización, modificación y actualización de la presente Política, se sancionará mediante un acto administrativo.

6. DIFUSIÓN:

- La versión del presente documento, así como toda la documentación vinculada al Sistema de Seguridad de la Información, será difundida a través de la Sección de Comunicaciones, por correo electrónico y en la **INTRANET del Servicio.**
- Para el personal que se incorpora a la Institución y para aquellos que cambian de calidad Jurídica, el Encargado(a) PMG del Sistema de Seguridad de la Información, realiza la Inducción, canalizado a través del Departamento Administrativo.
- Cada vez que SERVIU Metropolitano realice un proceso de contratación de servicio con algún proveedor, la Sección Adquisiciones del Departamento de Servicios Generales y las distintas áreas que elaboran las Bases de Licitación, deberán comunicar las Cláusulas de Confidencialidad de la Seguridad de la Información.

7. SANCIONES APLICABLES:

- El incumplimiento o violación a la Política de Seguridad de la Información y a toda la documentación vinculada al Sistema de Seguridad de la Información, debidamente acreditado, conllevará a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios(as) de SERVIU Metropolitano, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance del Sistema de Seguridad de la Información, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

8. EXCEPCIONES:

- Podrán existir casos particulares y debidamente justificados de exclusión parcial o total de lo estipulado en el presente documento, los que deberán ser aprobados por la Jefatura Superior del Servicio.
- Todas las excepciones, deberán ser formalmente registradas en un documento que emitirá y enviará el Encargado(a) de la Seguridad de la Información del Servicio, al Comité de Seguridad de la Información, para la toma de conocimiento.

9. DOCUMENTOS RELACIONADOS:

- Norma NCh-ISO 27001:2013 de Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.
- Resolución de Roles y responsabilidades de la Seguridad de la Información y su aplicación en el SERVIU Metropolitano.
- Política de Seguridad de la Información para las Relaciones con el Proveedor y su aplicación en el SERVIU Metropolitano.
- Instructivo Presidencial N° 008 /2018 de Ciberseguridad.

10. CONTROL DE VERSIONES:

N° Versión	Fecha Aprobación	Motivo de la revisión
05	21.12.2015	Resolución Exenta N° de fecha. Aprueba Integración de la versión N°05. Política General de Sistema de Seguridad de la Información del MINVU.
06	28.11.2017	Resolución Exenta N° de fecha. Aprueba Integración de la versión N°06. Política General de Sistema de Seguridad de la Información del MINVU.
08	15.09.2019	Aprueba Integración de la versión N°08. Política General de Sistema de Seguridad de la Información del MINVU.

Elaborado por:	- Encargado (a) PMG Seguridad de la Información.
Revisado por:	-**Coordinador(a) de SSI,** Jefe (a) Departamento Programación Física y Control. -**Encargado(a) Seguridad de la Información,** Subdirector(a) de Administración y Finanzas. **- Encargados(s) PMG Institucional.** **- Encargado(a) PMG Seguridad de la Información.** **- Encargados (as) de Activos.**

2. **ESTABLÉCESE** la obligación del Encargado(a) PMG de Seguridad de la Información del SERVIU Metropolitano, de difundir la presente Política, aprobada por esta Resolución Exenta y en coordinación con el Comité de Seguridad de la Información, velar por su estricto cumplimiento.

3. **DÉJESE SIN EFECTO** a contar de esta fecha, toda otra disposición que se contraponga a lo estipulado en esta Resolución.

4. **DÉJESE ESTABLECIDO,** que la presente Resolución no afecta el presupuesto del Servicio.

ANÓTESE, NOTIFÍQUESE, CÚMPLASE Y ARCHÍVESE.

CÉSAR FAÚNDEZ BURGOS
DIRECTOR
SERVIU METROPOLITANO

MURYS RAMÍREZ TAPIA
Ministro de Fe

GPZ/FBC/JES/CRS/MDS/EMA

DISTRIBUCIÓN:
- Dirección SERVIU Metropolitano.
- Subdirección de Administración y Finanzas.
- Subdirección de Pavimentación y Obras Viales.
- Subdirección de Vivienda y Equipamiento.
- Subdirección de Operaciones Habitacionales.
- Subdirección Jurídica.
- Departamento de Programación Física y Control.
- Departamento Administrativo.
- Departamento Servicios Generales.
- Contraloría Interna SERVIU Metropolitano.
- Sección Secretaría General / Ministro(a) de Fe SERVIU Metropolitano.
- Sección Informática.
- Sección Partes y Archivos.
- Sección Planificación.
- Encargado(a) PMG Sistema Seguridad de la Información.

Ministerio de Vivienda y Urbanismo

Gobierno de Chile

DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 10.265, (V. y U.), DE 2018, Y APRUEBA LA 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 SECRETARIAS REGIONALES MINISTERIALES).

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA
12 SEP 2019
RESOLUCION EXENTA
TRAMITADA

SANTIAGO, 12 SEP 2019 HOY SE RESOLVIO LO QUE SIGUE

RESOLUCIÓN EXENTA N° 2097 /

VISTOS: Lo dispuesto en el D.L N° 1.305, de 1975, que Reestructura y Regionaliza el Ministerio de Vivienda y Urbanismo; en el D.S N° 83, de 2005, 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° 10.265, (V. y U.), de 2018, que aprueba la Política General de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo; 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 se han dictado una serie de normas en materia de seguridad de la información, entre las que se encuentra el Decreto Supremo N° 83, de 2005, 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; 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 y el Instructivo Presidencial N° 008 de 2018, que imparte instrucciones en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los Órganos de la Administración del Estado.

b) La necesidad evaluada, como resultado de la revisión efectuada por parte del Comité de Seguridad de la Información, de reestructurar y ajustar contenidos en la Política General de Seguridad de la Información versión 07, aprobada mediante Resolución Exenta N°10.265, (V. y U.), de 2018.

RESOLUCIÓN:

I. Déjase sin efecto, a partir de la total tramitación del presente acto administrativo, la Resolución Exenta N°10.265, (V. y U.), de 2018.

II. Apruébase la Política General de Seguridad de la Información del MINVU, versión 08, para ser implementada en los 16 Servicios de Vivienda y Urbanización, en el Parque Metropolitano de Santiago, y en la Subsecretaría de Vivienda y Urbanismo (Nivel Central y las 16 Secretarías Regionales Ministeriales de Vivienda y Urbanismo), la que se detalla a continuación:

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRIGA
ABOGADA
DIVISIÓN JURÍDICA

Ministerio de Vivienda y Urbanismo

Gobierno de Chile

une la Ciudad

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE VIVIENDA Y URBANISMO

VERSIÓN 08

Contenido

0. GLOSARIO

Activo de Información	Todo elemento, sea tangible o no, que contenga datos que sean relevantes para el Ministerio, que se encuentren en formato físico o electrónico, sean equipos o aplicativos, o incluso las personas cuyo conocimiento sirve para los propósitos de la Institución.
Confidencialidad[1]	Propiedad de la información por la que no está disponible o divulgada a personas, entidades o procesos no autorizados.
Continuidad del Negocio	Persistencia de las operaciones de la institución.
Disponibilidad[1]	Propiedad de la información, que se traduce en que las personas o procesos autorizados puedan acceder a ella cuando lo requieran.
Documento de Aplicabilidad	Declaración documentada que describe los controles que son relevantes para el Sistema de Gestión de la Seguridad de la Información, en adelante, SGSI, de la organización y aplicables al mismo, así como el rol de cada institución del Ministerio de Vivienda y Urbanismo -en lo sucesivo, MINVU-, en la implementación de los controles de la norma ISO 27001:2013.
Incidente de Seguridad de la Información	Evento no deseado o inesperado que tiene una probabilidad significativa de comprometer las operaciones de la institución y amenazar la seguridad de la información.
Información	Toda comunicación o representación de conocimiento como datos, en cualquier forma, tales como formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea digital, en papel, audiovisual u otro.
Integridad[1]	Propiedad de mantener la información con exactitud y completitud.
Seguridad de la Información[1]	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Sistema de Gestión de Seguridad de la Información (SGSI)	La parte del sistema de gestión general, basada en un enfoque de riesgo organizacional, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Este incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

Nota: En el contenido del documento se identifican los cambios respecto a la versión anterior en negrita y cursiva.

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA
ABOGADA
DIVISIÓN JURÍDICA

[1] Fuente: ISO/IEC 27000:2018

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. DECLARACIÓN INSTITUCIONAL

El Ministerio de Vivienda y Urbanismo -MINVU- ha decidido establecer, implementar, mantener y mejorar continuamente un Sistema de Seguridad de la Información -en adelante el SSI-, siendo éste un *"compromiso en el fomento y desarrollo de una cultura de seguridad, basado en preservar los principios de confidencialidad, integridad y disponibilidad de la información y asegurar la continuidad operacional, en beneficio de los usuarios, ciudadanos y partes interesadas para alcanzar los objetivos institucionales, contribuyendo al desarrollo del país en los ámbitos de ciudad y territorio, barrio y vivienda".*

De este modo, la información es un activo esencial para que el MINVU alcance sus objetivos con el propósito de cumplir con su misión ministerial. Por tal motivo, entendemos por activo de información todos aquellos elementos que hacen posible o sustentan los procesos operativos o de negocio, como las personas que utilizan la información; los equipos, sistemas e infraestructura que soporta la información; y la información propiamente tal en cualquiera de sus múltiples formatos, incluyendo ***soporte*** papel y digital.

Para el desarrollo del SSI, la presente política general, las políticas específicas, procedimientos y otros documentos relacionados, se ajustan a los requerimientos normativos vigentes en seguridad de la información, además de considerar los aspectos pertinentes del marco normativo del MINVU[2].

2. OBJETIVO

El objetivo de este documento es:

- ***Establecer los lineamientos institucionales y entregar orientación en la implementación del Sistema de Seguridad de la Información del MINVU.***
- ***Definir los objetivos y principios para guiar las actividades relacionadas con la seguridad de la información, resguardando la confidencialidad, integridad y disponibilidad de sus activos relevantes, con el fin de mantener la continuidad operacional en los procesos de provisión de bienes y servicios estratégicos en concordancia con la normativa vigente en materias de Seguridad de la Información y Ciberseguridad de manera de cumplir eficientemente con los objetivos estratégicos del Ministerio de Vivienda y Urbanismo.***

2.1 Objetivos de la Seguridad de la Información

El Sistema de Seguridad de la Información del MINVU se alinea y permite soportar los objetivos estratégicos ministeriales definidos en la Ficha de Definiciones Estratégicas A0 [3], para lo cual cuenta con los siguientes objetivos de la gestión de seguridad de la información:

- Resguardar los activos de información mediante controles de seguridad aplicables a partir del análisis, evaluación y tratamiento de los riesgos que afecten su confidencialidad, integridad y disponibilidad.
- Asegurar la continuidad del negocio a través de acciones tendientes a gestionar los incidentes y a revertir y resolver contingencias que se detecten.

Para lo anterior, en el marco del SSI, se establecen un conjunto de lineamientos y prácticas de seguridad de la información en consistencia con las disposiciones indicadas en esta política en el punto 5, debiendo ser formalizadas a través de políticas específicas, procedimientos y otros documentos para su cumplimiento y aplicación por parte de las personas, especialmente en los procesos definidos en el alcance.

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA
ABOGADA
DIVISIÓN JURÍDICA

[2] Disponible en www.minvu.cl, enlace "Marco Normativo".

[3] Los objetivos estratégicos ministeriales se encuentran disponibles en la Ficha de Definiciones Estratégicas (Formulario A0) publicado en la Intranet del MINVU.

3. ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y DEL SSI – ALCANCE

La presente política es aplicable a los procesos asociados a los productos estratégicos que forman parte del SSI en cada Servicio[4] del MINVU.

Esta definición de procesos es formalizada/actualizada anualmente en cada Servicio por su respectivo Comité de Seguridad de la Información, quedando establecida dicha definición en el Acta de reunión.

Asimismo, esta política es aplicable a funcionarios de planta, contrata y honorarios, en adelante también "el personal", que forman parte del Ministerio de Vivienda y Urbanismo, o se relacionan con esta Secretaría de Estado, esto es, la Subsecretaría de Vivienda y Urbanismo (Nivel Central y sus 16 SEREMI), los 16 SERVIU y el Parque Metropolitano de Santiago, así como también a asesores, consultores, practicantes y personas naturales o jurídicas que prestan servicios para el MINVU.

Para el desarrollo del SSI, se consideran los requisitos de la norma NCh-ISO 27001:2013, así como los requisitos regulatorios y legales aplicables identificados en el documento Catastro Normativa MINVU.

La NCh-ISO 27001:2013 establece dominios y controles que se deben cumplir en el marco de un Sistema de Gestión de la Seguridad de la Información (SGSI). Estos dominios han sido considerados en el SSI del MINVU y corresponden a los siguientes:

1. *Políticas de Seguridad de la Información*
2. *Organización de la Seguridad de la Información*
3. *Seguridad ligada a los Recursos Humanos*
4. *Administración de Activos*
5. *Control de Acceso*
6. *Criptografía*
7. *Seguridad Física y del Ambiente*
8. *Seguridad de las Operaciones*
9. *Seguridad de las Comunicaciones*
10. *Adquisición, desarrollo y mantenimiento del Sistema*
11. *Relaciones con el Proveedor*
12. *Gestión de Incidentes de Seguridad de la Información*
13. *Aspectos de la Seguridad de la Información en la gestión de la continuidad del negocio*
14. *Cumplimiento*

Para estos dominios, se establecerá un conjunto de normas, directrices, procedimientos, instructivos y herramientas de seguridad que permitirán mitigar los riesgos que pudiesen afectar la protección de los activos de información. Esta documentación estará disponible para ***todo el personal del MINVU*** en la intranet institucional.

Esta Política genera el marco ministerial de Seguridad de la Información; sin embargo, cada Servicio tiene su propio sistema de Seguridad de la Información y puede definir las políticas específicas que considere necesarias y que sean de aplicación local; éstos documentos no pueden contener elementos que contravengan la presente política, aplicándose además esta última en todos los aspectos no regulados por aquellas.

Existen algunos controles que son abordados en forma transversal, que producto de la dependencia Tecnológica de SERVIU y PMS con la Subsecretaría de V. y U. se tratan desde Nivel Central. Para orientar al respecto el MINVU cuenta con un "Documento de Aplicabilidad", publicado en la Intranet, en el cual se identifican los controles de la norma ISO 27001:2013, su aplicabilidad institucional y el rol de la Subsecretaría, los SERVIU y el PMS en su implementación.

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA
ABOGADA
DIVISIÓN JURÍDICA

[4] El término "Servicio" hace referencia a la Subsecretaría de Vivienda y Urbanismo (Nivel central y 16 SEREMI), a 16 SERVIU y al Parque Metropolitano de Santiago (PMS).

4. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades para el SSI son definidos por cada Servicio, en cuanto al contenido específico de su composición y funciones, mediante la formalización de un acto administrativo que considera al menos:

- **Encargado/a de Seguridad de la Información**: en cuyo rol el Jefe de cada Servicio delega las decisiones relativas a la seguridad de la información y su coordinación, asegurando la alineación del SSI y sus objetivos al cumplimiento de los objetivos estratégicos, coordinando las acciones necesarias para satisfacer los requisitos aplicables, favoreciendo la ***mejora continua del sistema*** y la satisfacción de las partes interesadas. ***Este Encargado/a es responsable de la correcta aplicación de esta política y su periódica revisión.***
- **Comité de Seguridad de la Información**, o Comité de similar denominación: formado por un equipo multidisciplinario de cada Servicio que tiene injerencia en las decisiones estratégicas relativas a la seguridad de la información, a partir de los dominios que regulan los diferentes aspectos.

Cabe destacar que los usuarios, funcionarios de planta, contrata y honorarios que forman parte del Ministerio de Vivienda y Urbanismo, así como también asesores, consultores, practicantes y personas naturales o jurídicas que prestan servicios para el MINVU, ***son responsables de cumplir*** las políticas de seguridad de la información del MINVU, asegurar la ***confidencialidad***, disponibilidad e integridad de la información que tienen a su cargo y reportar oportunamente los incidentes de seguridad de la información ***que detecten en el desarrollo de sus funciones.***

5. DISPOSICIONES PARA RESGUARDAR LOS ACTIVOS DE INFORMACIÓN

La seguridad de la información es el conjunto de medidas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger los activos de información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.
A continuación, se describe cómo el MINVU aborda estos principios básicos de Seguridad de la Información:

5.1 De la confidencialidad de los activos de información

El MINVU se compromete a preservar la confidencialidad de la información institucional, estableciendo lineamientos, prácticas de seguridad y mecanismos para clasificar y reconocer la información de carácter confidencial en la gestión interna, que deba ser protegida ante filtración o divulgación no autorizada. Esta clasificación es de carácter interna y diferente de la tipificación del carácter reservado de la información, la cual se encuentra a cargo del equipo de Transparencia en cada Servicio, quienes resguardan el principio de transparencia de la función pública[5] recogido en la Ley N° 20.285 sobre Acceso a la Información Pública.

Por lo anterior, y dada la condición pública de la información elaborada con presupuesto de la nación y que obra en poder de los Órganos de la Administración del Estado, es importante señalar que su resguardo no implica desconocimiento ni obstaculización del derecho de toda persona a solicitar y recibir información, en la forma y condiciones que establece la Ley N° 20.285.

Además, el resguardo de la información involucra la obligación de las personas que trabajan en el tratamiento de datos personales o que tengan acceso a estos, de guardar secreto sobre los mismos, según lo dispone la Ley N° 19.628 de Protección de Datos de Carácter Personal.

De este modo, cada Servicio se compromete a implementar los controles necesarios para garantizar que, tanto la información física como la digital, sea accesible sólo por aquellos usuarios autorizados y de acuerdo a la legislación vigente, revisando periódicamente estos lineamientos.

5.2 De la integridad de los activos de información

El MINVU establece lineamientos, prácticas de seguridad y mecanismos que resguardan la integridad de los activos de información contenida en cualquier espacio, equipo, sistema o infraestructura, en todos los formatos posibles, salvaguardando además la mayor completitud, coherencia, consistencia y

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA ARAGADA
DIVISIÓN JURÍDICA

[5] Artículo 5 de la Ley 20.285, que establece el carácter público de la información de los órganos de la Administración del Estado.

actualización de sistemas y procesos.

5.3 De la disponibilidad de los activos de información

EL MINVU asegura la disponibilidad de los activos de información ministerial, incluyendo la disponibilidad de equipos, sistemas e infraestructura que la contengan o la provean en los niveles y tiempos requeridos, tanto a escala interna como externa, estableciendo lineamientos, prácticas de seguridad y mecanismos que prevengan cualquier acción que elimine o exponga la información relevante y que mantengan la continuidad del flujo de información.

6. DISPOSICIONES PARA ASEGURAR LA CONTINUIDAD DEL NEGOCIO

El MINVU busca asegurar que la comunidad vinculada disponga de los servicios e información, de manera oportuna y cuando esta sea requerida según la normativa vigente. Para ello procura que los servicios otorgados a las personas sean resguardados y recuperados en forma adecuada y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento o equipamiento de procesamiento.

7. GESTIÓN DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

7.1 Generación de una política y otros documentos

Las políticas de seguridad de la información se elaboran en base a un formato tipo establecido para dicho propósito publicado en ***la columna*** Trabajo Colaborativo SSI en la Intranet institucional. Asimismo, para la implementación operativa de algunas políticas específicas de seguridad, se elaboran procedimientos u otros instrumentos que se alinean con los parámetros establecidos de documentación en cada Servicio.

7.2 Aprobación de una política y otros documentos

Las políticas específicas de seguridad son aprobadas a través de resolución del Jefe de Servicio, ***facultad que no puede ser delegada.***

Otros documentos como normativas, procedimientos e instructivos son aprobados a través de un acto administrativo (Resolución) del Jefe de Servicio, ***o por aquellos funcionarios en quienes haya sido delegada dicha atribución***, dependiendo de los lineamientos y prácticas de seguridad particulares o transversales ***definidos en cada Servicio***, conforme a su estructura y requerimientos de seguridad.

7.3 Difusión de una política y otros documentos

Las versiones vigentes de la presente política y aquella documentación vinculada al Sistema de Seguridad de Información se publica de acuerdo a lo establecido por cada Servicio, asegurando que el contenido de la documentación sea accesible y comprensible para todo ***el personal del MINVU***.

La difusión de la presente política, las políticas específicas de seguridad, los procedimientos y otros documentos, se efectúa a través de los canales de difusión establecidos, pudiendo utilizarse publicación en la Intranet institucional y/o Minvuletín y/o Correo electrónico y/o Afiches y/o volantes, u otro medio que la institución considere pertinente.

7.4 Revisión de la política

La presente política será revisada anualmente o cuando ***el/la Encargado/a de Seguridad de la Información de uno o más Servicios 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 en el ambiente técnico, recomendaciones realizadas por autoridades pertinentes, tendencias relacionadas con amenazas y vulnerabilidades, entre otras.

Asimismo, cada Servicio evaluará el cumplimiento de la presente política general, a lo menos cada tres años, mediante auditorías internas, externas y/o revisiones independientes.

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA MO
ABOGADA
DIVISIÓN JURÍDICA

8. SANCIONES APLICABLES

El incumplimiento o violación a esta política, conlleva, en el caso de funcionarios del MINVU, ***la aplicación de alguna de las medidas disciplinarias previstas en el Estatuto Administrativo (censura, multa, suspensión o destitución), previa sustanciación del respectivo proceso disciplinario y en la medida que se acredite en el marco del mismo, responsabilidad administrativa por incumplimiento o violación de esta política; o el término anticipado del contrato por incumplimiento de las obligaciones que el mismo contempla, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política.*** Lo anterior, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

9. CONTROL DE VERSIONES

Versión	Fecha Aprobación	Motivo de la revisión	Autor(es)
06	Octubre 2017	Revisión anual, considera nuevos requerimientos Red de Expertos. Se identifican los cambios en negrita y cursiva.	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Claudio Paredes/ Jefe de Ingeniería y Explotación de Sistemas DINFO; Ivonne Valdivia / Profesional Depto. Estudios DIVAD; Viviana Peña / Analista Sección Gestión de Procesos DIFIN; Marcela Jara/ Encargada Sección Gestión de Procesos DIFIN.
07	Octubre 2018	Revisión anual, considera ajuste en la aprobación de documentos por observación formulada por Contraloría General de la República. Se identifican los cambios en negrita y cursiva.	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Claudio Paredes/ Jefe de Ingeniería y Explotación de Sistemas DINFO; Ivonne Valdivia / Profesional Depto. Estudios DIVAD; Marcela Jara/ Encargada Sección Gestión de Procesos DIFIN.
08	Julio 2019	Revisión anual, considera ajuste en la aprobación de documentos y algunas especificaciones por recomendación de Red de Expertos. Se identifican los cambios en negrita y cursiva.	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Claudio Paredes/ Jefe de Ingeniería y Explotación de Sistemas DINFO; Ivonne Valdivia / Profesional Depto. Estudios DIVAD; Marcela Jara/ Analista Dpto. de Planificación y Control de Gestión DIFIN; M. Paula Melis Otonel/ Contralora Interna SERVIU Araucanía.

Revisión:	Guillermo Rolando Vicente/ Subsecretario de Vivienda y Urbanismo. Marcela Acuña Gómez/ Jefa Gabinete Subsecretaría – Encargada de Seguridad de la Información. Andrea Ubal Espinoza / Jefe Sección Control de Gestión DIFIN. Comité de Seguridad de la Información Subsecretaría de V. y U. Encargados/as de Seguridad de la Información de SERVIU y Parque Metropolitano.
Aprobación:	Cristián Monckeberg Bruner / Ministro de Vivienda y Urbanismo.

MINISTERIO DE VIVIENDA Y URBANISMO
CARMEN GLORIA BARRERA
ABOGADA
DIVISIÓN JURÍDICA

III. Establécese la obligación de los/as Encargados/as de Seguridad de la Información de la Subsecretaría de V. y U., los SERVIU y el Parque Metropolitano de Santiago de efectuar la difusión de la política fijada por este instrumento a todos los equipos de trabajo, así como realizar todas las acciones tendientes a su implementación y velar por su estricto cumplimiento.

IV. Se deja constancia que la presente Resolución no irroga gastos para el presupuesto de este Ministerio, ni para los Servicios que se relacionan con el Gobierno por su intermedio.

ANÓTESE, NOTIFÍQUESE, CÚMPLASE Y ARCHÍVESE.

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIO

MINISTERIO DE VIVIENDA Y URBANISMO
DIVISIÓN JURÍDICA
CARMEN GLORIA RABRERA ARCEDA

CRISTIAN MONCKEBERG BRUNER
MINISTRO DE VIVIENDA Y URBANISMO

Ministerio de Vivienda y Urbanismo
Gabinete del Ministro
MINISTRO

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

GRV/MAG/CPL/AGG/CEV/PHN/AUE

DISTRIBUCIÓN:
- Gabinete Ministro V. y U.
- Gabinete Subsecretario V. y U.
- SEREMI (16)
- Directores SERVIU (16)
- Director PMS
- Divisiones Nivel Central (7)
- Auditoría Interna Ministerial
- Contraloría Interna Ministerial
- Coordinador Nacional Programa Reconstrucción
- Programa Aldeas y Campamentos
- Sistema Integrado de Atención a la Ciudadanía (SIAC)
- Depto. Comunicaciones
- Comisión de Estudios Habitacionales y Urbanos (CEHU)
- Depto. Planificación y Control de Gestión DIFIN

MINISTERIO DE VIVIENDA Y URBANISMO
GABINETE MINISTRO

GUILLERMO ROLANDO VICENTE
SUBSECRETARIO DE VIVIENDA Y URBANISMO

03

2 DE FEBRERO DE 2021

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

SERVIU METROPOLITANO

A.15.01.01
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR

NORMA NCH-ISO 27001:2013

Subdirección de Administración y Finanzas
Sistema de Seguridad de la Información
OFPA N° 15

ACTUALIZA Y COMPLEMENTA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR Y SU APLICACIÓN EN SERVIU METROPOLITANO.

CON ESTA FECHA SE HA DICTADO LA SIGUIENTE:
RESOLUCIÓN EXENTA Nº _____/
SANTIAGO,

3726 19.11.2020

VISTOS:

a. Lo dispuesto en la Ley Nº 18.575 de 1986, Orgánica Constitucional de Bases Generales de la Administración del Estado, el Decreto Supremo Nº 355/1976 (V. y U.) Reglamento Orgánico de los Servicios de Vivienda y Urbanización; y el Decreto Ley Nº 1305, que reestructura y regionaliza el Ministerio de la Vivienda y Urbanismo, de 1975;

b. Lo dispuesto en el Decreto Nº 83/2004 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;

c. Lo dispuesto en la Ley Nº 20.285 de 2009, sobre Acceso a la Información Pública y el Decreto Nº 13 de 2009, ambos del Ministerio Secretaría General de la Presidencia;

d. Lo dispuesto en la Ley Nº 19.628 de 1999, sobre Protección de la vida Privada o Protección de datos de carácter personal;

e. Lo dispuesto en la Ley Nº 19.886/2003 de Bases sobre Contratos Administrativos de Suministros y Prestación de Servicios, y el Decreto N° 250/2004 del Ministerio de Hacienda, que aprueba el Reglamento de la Ley Nº 19.886/2003, y sus modificaciones legales;

f. Lo dispuesto en la Norma NCh-ISO 27001:2013 de Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información – Requisitos;

g. El Instructivo Presidencial Nº 008 de fecha 23 de octubre de 2018, que imparte Instrucciones urgentes en materia de Ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado;

h. La Resolución Exenta Nº 5091 de fecha 30 de octubre de 2019, que aprueba la Política de Seguridad de la Información para las Relaciones con el Proveedor y su aplicación en SERVIU Metropolitano;

i. La Resolución Exenta Nº 2663 de fecha 21 de agosto de 2020, que actualiza y complementa la Estructura, Roles y Responsabilidades del Comité de Seguridad de la Información en SERVIU Metropolitano;

j. La Resolución Nº 7 y 8, de fecha 26/03/2019 y 27/03/2019, respectivamente, de la Contraloría General de la República, que Fija Normas sobre Exención del trámite de Toma de Razón, y que determina los montos en unidades tributarias mensuales, a partir de los cuales los actos que se individualizan quedarán sujetos a Toma de Razón o Controles de Reemplazo cuando corresponda;

k. La Resolución Exenta RA Nº 272/1310/2020 (V. y U.) de fecha 03 de julio de 2020, que me nombra Directora del Servicio de Vivienda y Urbanización Metropolitano, y las facultades que en tal carácter me competen en conformidad al D.S Nº 355 (V. y U.) del año 1976, Reglamento Orgánico de los SERVIU:

CONSIDERANDO:

a. La necesidad de actualizar y complementar la Política de Seguridad de la Información para las Relaciones con el Proveedor, señalado en el visto h), para su aplicación en SERVIU Metropolitano, motivo por el cual, dicto la siguiente:

RESOLUCIÓN:

1. **APRUÉBASE,** la actualización, aplicación y difusión de la Política de Seguridad de la Información para las Relaciones con el Proveedor, que se define a continuación y aplíquese íntegramente partir de la fecha en que sea formalizada la presente Resolución Exenta, en SERVIU Metropolitano.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR

1. OBJETIVO:

- Establecer el marco normativo para la contratación de servicios externos, en relación a la Seguridad de la Información para los Proveedores que prestan servicio al SERVIU Metropolitano, en el desarrollo de sus funciones y que puedan tener acceso a la información, sistemas de información y/o recursos en general, con el fin de proteger la confidencialidad, Integridad y disponibilidad de la Información y sistemas propios del Servicio.

2. ALCANCE:

- Esta Política será aplicable a todos los Proveedores que prestan servicios en el SERVIU Metropolitano, y/o vinculados a través de un Contrato de Provisión de Servicios, que, para su desempeño, acceden a todos los tipos de información, independientemente del formato, ya sean documentos en papel o electrónicos, aplicaciones y bases de datos, los que deberán conocer y comprender.
- Para efectos de la aplicación de la presente Política, se entenderá como activo de información, toda información, personas, tecnología y equipamiento que la soportan y a todos los procesos de provisión de bienes y servicios definidos en el Formulario A1 de las Definiciones Estratégicas.
- Esta Política está relacionado con el cumplimiento del Control A.15.01.01 de la Norma NCh-ISO 27001:2013, sobre Política de Seguridad de la Información para las Relaciones con el Proveedor.

3. ROLES Y RESPONSABILIDADES:

- Los roles y responsabilidades del Comité de Seguridad de la Información, del SERVIU Metropolitano, son los siguientes:

Cargos Responsables	Roles Claves
- **Director(a) SERVIU Metropolitano.**	1. Designar a los responsables del proceso del Sistema de Seguridad de la Información, en el Servicio; 2. Sancionar las Políticas y Estrategias diseñadas para gestionar la Seguridad de la Información en el Servicio.
- **Encargada(o) de Seguridad de la Información.** - Subdirector(a) de Administración y Finanzas.	1. Aprobar toda la documentación que genera el Sistema de Seguridad de la Información, en el Servicio; 2. Supervisar y velar por el cumplimiento e implementación del proceso de Seguridad de la Información en SERVIU Metropolitano.

Cargos Responsables	Roles Claves
- **Coordinador(a) de Seguridad de la Información.** - Encargado(a) Sección Control de Gestión SDAF.	1. Presidir las reuniones del Comité de Seguridad de la Información; 2. Coordinar las reuniones periódicas que realice el Comité de Seguridad de la Información; 3. Validar las Actas y acuerdos que se generen, producto de las reuniones periódicas que efectúe el Comité de Seguridad de la Información; 4. Gestionar la aprobación de Políticas, con Encargada(o) de Seguridad de la Información del Servicio; **5.** Coordinar el cumplimiento de los controles comprometidos y sus respectivos verificadores, con Analista Control de Gestión SDAF.
- **Analista Control de Gestión SDAF**	1. Actualizar la documentación de los controles transversales comprometidos por el Ministerio de Vivienda y Urbanismo y que se integran al SERVIU Metropolitano; 2. Realizar y dirigir las reuniones con las Encargadas(os) de Activos y Encargados(as) de Incidentes del Sistema de Seguridad de la Información; 3. Solicitar trimestralmente a los Encargados(as) de Activos, los registros de Operación de todos los controles comprometidos, en el Sistema Seguridad de la Información; 4. Elaborar Procedimientos y/o documentación para el cumplimiento de los controles del Sistema de Seguridad de la Información; 5. Informar al Comité de Seguridad de la Información, la documentación vigente y actualizada del proceso de Seguridad de la Información; 6. Reportar al Encargado(a) de Seguridad de la Información y a la Encargada(o) Sección Gestión y Calidad, los controles comprometidos para su implementación en el Servicio; 7. Difundir a través de la Sección de Comunicaciones del Servicio, las Políticas y Procedimientos implementados, del Sistema de Seguridad de la Información; 8. Realizar el seguimiento mensual de todos los controles comprometidos, en el Sistema Seguridad de la Información; 9. Informar mensualmente a la Coordinadora de Seguridad de la Información, el estado de todos los controles; 10. Registrar y resguardar los documentos “Actas y acuerdos” que se levanten, producto de las reuniones periódicas que efectúa el Comité de Seguridad de la Información; 11. Diseñar el Programa para la Charla o Taller de Inducción en Seguridad de la Información.

Cargos Responsables	Roles Claves
- **Encargado(a) Sección Gestión y Calidad.**	1. Monitorear el reporte periódico del avance de los controles comprometidos y entregados por Analista Control de Gestión SDAF; 2. Revisar las Políticas y Procedimientos del Sistema de Seguridad de la Información; 3. Revisar y validar procedimientos del Sistema de Seguridad de la Información vinculados al Sistema de Gestión de la Calidad; 4. Participar en las reuniones del Comité de Seguridad de la Información; **5.** Participar en las reuniones que realiza el Ministerio de Vivienda y Urbanismo, para tratar temas de Seguridad de la Información.
- **Encargada(o) Activos de Información Físicos.** - Ministro de Fe	1. Participar en la eliminación segura de los activos de Información Físicos; 2. Participar en las reuniones del Comité de Seguridad de la Información.
- **Encargado(a) Activos de Información Físicos.** - Encargada(o) Sección Partes y Archivos.	1. Participar en la elaboración de las Políticas y Procedimientos propios de la Sección Partes y Archivos; 2. Participar en la revisión de Políticas específicas y documentos relacionados al Sistema de Seguridad de la Información, de la Sección Partes y Archivos.
- **Encargado(a) Gestión de las Personas para la Seguridad de la Información.** - **Encargada(o) Infraestructura para la Seguridad de la Información.** - **Encargado(a) Reportes y Registros de Incidentes de Seguridad de la Información.** - Jefe(a) Departamento Administrativo. - Encargada(o) de Equipo de Prevención de Riesgos.	1. Participar en la elaboración de las Políticas y Procedimientos propios del Departamento Administrativo; 2. Participar de la revisión de Políticas específicas y de los documentos relacionados con el Sistema de Seguridad de la Información, del respectivo Departamento Administrativo; 3. Desarrollar, documentar y mantener las Políticas de Seguridad propias de su área y velar por su correcta aplicación en el SERVIU Metropolitano; 4. Gestionar la confección de Planes de Continuidad para actuar frente a contingencias; 5. Coordinar con las áreas correspondientes, las instancias necesarias para activar los Planes de Continuidad en el Servicio; 6. Realizar las gestiones con las áreas correspondientes, que permitan recuperar las operaciones normales del Servicio; 7. Planificar, gestionar y evaluar pruebas, simulacros y ejercicios de contingencia; 8. Reportar, registrar, solucionar y escalar Incidentes de Seguridad de la Información, informando al Encargado(a) de Seguridad de la Información y al Analista Control de Gestión SDAF.

Cargos Responsables	Roles Claves
- **Encargada(o) Activos de Información Digitales.** - **Encargado(a) Infraestructura para la Seguridad de la Información.** - **Encargada(o) Reportes y Registros de Incidentes de Seguridad de la Información.** - Encargado(a) Sección Informática.	1. Participar en la elaboración de las Políticas y Procedimientos propios de la Sección de Informática; 2. Desarrollar, documentar y mantener las Políticas de Seguridad de la Información, en el ámbito Informático, velando por su correcta aplicación en el SERVIU Metropolitano; 3. Liderar las soluciones otorgadas a los Incidentes de Seguridad de la Informática; 4. Participar en las reuniones de Comité de Seguridad de la Información; 5. Validar y proponer al Analista Control de Gestión SDAF, los planes de contingencia para asegurar la Continuidad de Operaciones Informáticas críticas de la Institución; 6. Controlar e investigar Incidentes y/o violaciones de Seguridad Informática e informar oportunamente a las Jefaturas del Servicio y al Analista Control de Gestión SDAF, de la situación detectada; **7.** Reportar, registrar, solucionar y escalar Eventos e Incidentes de Seguridad de la Información, informando de ello a la Encargada(o) de Seguridad de la Información y al Analista Control de Gestión SDAF.
- **Encargado(a) Infraestructura para la Seguridad de la Información.** - **Encargada(o) Reportes y Registros de Incidentes de Seguridad de la Información.** - Jefa(e) Departamento Servicios Generales. -	1. Participar en la elaboración de las Políticas y Procedimientos propios del Departamento de Servicios Generales, del Servicio; 2. Desarrollar, documentar y mantener las Políticas de Seguridad propias de su área y velar por su correcta aplicación en el SERVIU Metropolitano; 3. Validar y proponer al Analista Control de Gestión SDAF, los planes de contingencia para asegurar la Continuidad de Operaciones críticas de la Institución; 4. Reportar, registrar, solucionar y escalar Eventos e Incidentes de Seguridad de la Información, informando de ello al Encargado(a) de Seguridad de la Información y al Analista Control de Gestión SDAF; 5. Realizar las gestiones con las áreas correspondientes que permitan recuperar las operaciones normales del Servicio; 6. Comunicar y difundir los alcances correspondientes, sobre la Política de Seguridad de Información para las Relaciones con el Proveedor.

4. DEFINICIONES:

- Para implementar este control en el SERVIU Metropolitano, se deberán aplicar las siguientes directrices:

4.1 Cumplimiento del Contrato:

a. Se entenderá que todas las actividades desarrolladas por los proveedores que prestan servicios a SERVIU Metropolitano, se encuentran establecidas en los respectivos contratos de provisión de servicios que se vinculan a este.

b. Las actividades desarrolladas por proveedores se realizarán de acuerdo a lo establecido en los procesos correspondientes: Bases de Licitación, Términos de referencias, Contrato de Provisión y Orden de compra, que se vinculan a este.

c. De acuerdo a lo establecido en las cláusulas asociadas al contrato de provisión de servicios, todo proveedor que desarrolle labores para SERVIU Metropolitano deberá cumplir con lo definido en las Políticas y Procedimientos del Sistema de Seguridad de la Información de SERVIU Metropolitano.

d. El intercambio de información que se produzca entre SERVIU Metropolitano y las empresas Proveedoras se entenderá que han sido realizados dentro del marco establecido por el proceso correspondiente. Esta información no podrá ser utilizada en ningún caso para fines diferentes a los asociados a dicho contrato.

4.2 Accesos a Equipos de Tecnologías de la Información (TI):

a. Las instalaciones de sistemas, equipos de comunicación y/o programas en los computadores deben ser autorizados por la Sección Informática del Servicio.

b. Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de información propia del Servicio sin la debida autorización.

c. El Proveedor se compromete a utilizar los recursos dispuestos dentro de la Institución para la provisión del servicio, de acuerdo a las condiciones establecidas en cada uno de los procesos.

d. Las contraseñas entregadas por la Sección Informática a los Proveedores para acceso a los equipos computacionales o sistemas Institucionales, son de carácter confidencial, personal e intransferible.

e. Los recursos que SERVIU Metropolitano entrega a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, materiales, herramientas e implementos de seguridad y sanitarios, etc.), están disponibles exclusivamente para complementar las obligaciones y el propósito de la operativa para los fines as que fueron proporcionados. La Sección Informática y el Departamento de Servicios Generales implementarán mecanismos de control, con la finalidad de verificar el uso adecuado de estos.

f. Los equipos computacionales propios de los proveedores deben ser compatibles con los estándares solicitados por la Sección Informática y serán conectados a la red institucional previa autorización de dicha Sección, los que estarán a disposición para la instalación del Software homologado y las configuraciones apropiadas de acuerdo al contrato.

g. Durante la ejecución de trabajos en las distintas dependencias de SERVIU Metropolitano por parte de las distintas empresas contratistas y subcontratistas, es responsabilidad de la Inspección Técnica de Obras y/o de la Comisión Técnica establecida, del Administrador del Contrato y/o de la Unidad correspondiente a cargo de los trabajos, informar y establecer las coordinaciones y autorizaciones correspondientes, a fin de que se establezcan los controles definidos para cautelar el cumplimiento de las distintas disposiciones legales y las respectivas supervisiones técnicas que limiten el libre acceso a las áreas donde se maneje y resguarde información, equipos y bienes, sensibles del Servicio.

h. El proveedor sólo podrá utilizar las carpetas compartidas conectadas a la red institucional y que hayan sido aprobadas por la Sección Informática para el desempeño de su trabajo, todas las informaciones contenidas en dichas carpetas deberán ser entregadas a su contraparte técnica Institucional, para luego ser eliminadas del equipo computacional. El proveedor nunca podrá crear carpetas temporales en unidades locales del equipo computacional asignado por el Servicio.

i. El proveedor sólo considerará como información no confidencial aquella a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos para tal efecto por SERVIU Metropolitano

4.3 Confidencialidad de la Información:

a. Los Proveedores que presten servicios al SERVIU Metropolitano y que se encuentren físicamente en nuestras dependencias deberán conocer y cumplir con la Política de Seguridad de la Información disponible en la Página Web del SERVIU Metropolitano (www.serviurm.cl).

b. El Proveedor que tiene acceso a información del SERVIU Metropolitano deberá considerar que dicha información siempre tendrá el carácter de confidencialidad, y no podrán ser difundidas, a excepción que existan cláusulas específicas en el contrato.

c. El Proveedor que tenga acceso a la información confidencial durante la prestación del contrato, contenida en los sistemas computacionales, documentada e impresas, deberá entender que dicha información es estrictamente confidencial y sin que ello le confiera derecho alguno de posesión, titularidad o copia de estas.

d. Las empresas contratistas y subcontratistas que ejecuten trabajos en las distintas dependencias de SERVIU Metropolitano, no podrán acceder a las distintas áreas del Servicio sin previa autorización de su contraparte técnica (Inspección Técnica de Obras, Comisión Técnica, Administrador del Contrato o Unidad correspondiente), y sólo podrán realizar el trabajo encomendado en el área asignada, sin acceder a información, equipos y bienes allí disponibles.

e. El Proveedor deberá guardar absoluta confidencialidad sobre los antecedentes reservados o no, que pongan a su disposición SERVIU Metropolitano y, en general, de todos aquellos que conozca con ocasión de la ejecución de los servicios. El proveedor deberá garantizar el resguardo de la confidencialidad de la información señalada precedentemente, reservándose el SERVIU Metropolitano el derecho de ejercer las acciones legales que correspondan de acuerdo a las normas legales vigentes.

f. La divulgación, por cualquier medio, de la información antes referida por parte del proveedor, durante la vigencia del contrato, o después de su finalización, dará lugar al SERVIU Metropolitano para entablar las acciones judiciales que correspondan, sin perjuicio de la responsabilidad solidaria por los actos que hayan ejecutado sus empleados y quienes resulten responsables.

g. Toda información, datos, documentos y registros, que los integrantes de su equipo de trabajo, sus dependientes u otras personas vinculadas a él, conozcan o llegaren a conocer con ocasión o a propósito del contrato y sus actividades complementarias, se tratarán como información confidencial y propiedad intelectual del SERVIU. El proveedor no podrá hacer uso de la información excepto que esté expresamente autorizado por el SERVIU, y ajustándose en todo caso a las disposiciones de la Ley Nº 19.628, sobre protección de la vida privada o protección de datos de carácter personal. El incumplimiento de esta obligación autorizará al SERVIU para poner término anticipado al contrato y dará lugar a la interposición de las acciones judiciales que correspondan.

5. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN:

- La evaluación y revisión del presente documento, así como toda la documentación vinculada al Sistema de Seguridad de la Información, deberá efectuarse, al menos, una vez al año por el Comité de Seguridad de la Información (CSI), o a solicitud de la Jefatura superior del Servicio. Así mismo, frente a un cambio de contexto de la Institución, deberá asegurar su continuidad, idoneidad y confiabilidad al respecto.
- La formalización, modificación y actualización de la presente documentación, se sancionará mediante un acto administrativo.

6. DIFUSIÓN:

- La versión del presente documento, así como toda la documentación vinculada al Sistema de Seguridad de la Información, será difundida a través de la Sección de Comunicaciones, por correo electrónico y publicada en la INTRANET y en el Sitio Web del Servicio.
- Para el personal que se incorpora a la Institución y para quienes se cambian de calidad Jurídica, el o la Analista Control de Gestión SDAF, les proporcionará la necesaria Inducción, canalizado a través del Departamento Administrativo.
- Cada vez que SERVIU Metropolitano realice un proceso de contratación de servicio con alguna entidad proveedora, la Sección Adquisiciones del Departamento de Servicios Generales, según sea el caso, deberá comunicar, difundir y publicar las Cláusulas de Confidencialidad de la Información.
- En el caso que se licite la ejecución de una Obra al interior de las dependencias del Servicio, la Sección Propuestas mencionará en la adición de las Bases, la existencia de la Política del Sistema de Seguridad de la Información, para conocimiento de todos los oferentes.
- Al momento de realizar la contratación de una Obra al interior de las dependencias del Servicio, el área Encargada de realizar esta gestión, deberá comunicar, difundir y publicar las Cláusulas de Confidencialidad de la Información en la Resolución de Contrato.

7. SANCIONES APLICABLES:

- El presente documento tiene su base en las definiciones, términos y controles descritos en la Norma Chilena NCh-ISO 27001:2013 y en los requisitos legales, normativos y contractuales relativos a la Seguridad de la Información, que sean aplicables a la Organización.
- El incumplimiento o violación a toda documentación vinculada al Sistema de Seguridad de la Información, debidamente acreditado, conllevará a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto al personal del SERVIU Metropolitano, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance del Sistema de Seguridad de la Información, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.
- El personal externo deberá garantizar el cumplimiento de las restricciones legales al uso de información confidencial. En caso de incumplimiento o mal uso de la información o de cualquiera de estas obligaciones, serán sancionadas de acuerdo a lo establecido en las Normas Legales del Servicio y a los procedimientos asociados a cada una de las áreas de negocios.

8. EXCEPCIONES:

- Podrán existir casos particulares y debidamente justificados de exclusión parcial o total de lo estipulado en el presente documento, los que deberán ser aprobados por la Jefatura Superior del Servicio.
- Todas las excepciones, deberán ser formalmente registradas en un documento que emitirá y enviará el Encargado(a) de la Seguridad de la Información del Servicio al Comité de Seguridad de la Información, para la toma de conocimiento.

9. DOCUMENTOS RELACIONADOS:

- La Ley Nº 19.886/2003. Ley de Bases sobre contratos administrativos de suministro y prestación de Servicios.
- La Ley Nº 16.744/1968. Establece Normas Sobre Accidentes del Trabajo y Enfermedades Profesionales.
- La Ley Nº 20.123/2006. Regula el Trabajo en Régimen de Subcontratación, el funcionamiento de las Empresas de servicios transitorios y el contrato de Trabajo de servicios transitorios.

- La Ley Nº 19.628 / agosto 1999. Sobre Protección de la vida Privada. Ministerio Secretaría General de la Presidencia.
- La Ley Nº 20.285/ agosto 2008. Sobre Acceso a la Información Pública. Ministerio Secretaría General de la Presidencia.
- Decreto N° 236/2002. Aprueba Bases Generales Reglamentarias de Contratación de Obras para Los Servicios de Vivienda y Urbanización
- NCh-ISO 27001:2013 de Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.
- Política General para la Seguridad de la Información y su aplicación en el SERVIU Metropolitano.
- Política de Control de Acceso Físico y su aplicación en el SERVIU Metropolitano.
- Política de Control de Acceso Lógico y su aplicación en el SERVIU Metropolitano.
- Procedimiento Supervisión y Revisión de los Servicios del Proveedor, P-SSI-15 del SERVIU Metropolitano.
- Procedimiento de Compras, P-SCC-001/2016 del SERVIU Metropolitano.
- Procedimiento Informe de Eventos de Seguridad de la Información, del Ministerio de Vivienda y Urbanismo.

10.CONTROL DE VERSIONES:

N° Versión	Fecha Aprobación	Motivo de la revisión
00	28.11.2017	Resolución Exenta N° 6602 de fecha 28.11.2017. Aprueba la Política de Seguridad de la Información para las Relaciones con el Proveedor y su aplicación en el SERVIU Metropolitano.
01	30.10.2019	Resolución Exenta N° 5091 de fecha 30.10.2019. Actualiza y Complementa Política de Seguridad de la Información para las relaciones con el Proveedor y su aplicación en SERVIU Metropolitano.
02	25.09.2020	Actualiza y complementa Política de Seguridad de la Información para las relaciones con el Proveedor y su aplicación en SERVIU Metropolitano.

Elaborado por:	**- Analista Control de Gestión SDAF.**
Revisado por:	**- Encargado(a) Seguridad de la Información.** - Subdirector(a) Administración y Finanzas. **- Coordinador(a) de Seguridad de la Información.** - Encargado(a) Sección Control de Gestión SDAF. **- Encargada(o) Sección Gestión y Calidad.** **- Encargados(as) de Activos.** **- Analista Control de Gestión SDAF.**

2. **APRUÉBASE,** las Cláusulas de Confidencialidad de la Información, las que deberán ser comunicadas, difundidas y publicadas por la Sección Adquisiciones del Depto. de Servicios Generales y la Sección Propuesta del Depto. de Programación Física y Control, según sea el caso, para cada proceso de contratación de servicio con algún Proveedor.

3. **ESTABLÉZCASE,** al Analista Control de Gestión SDAF del SERVIU Metropolitano, de difundir la presente Política, aprobada por esta Resolución Exenta y en coordinación con el Comité de Seguridad de la Información, velar por su estricto cumplimiento.

4. **DÉJESE SIN EFECTO,** a contar de esta fecha, toda otra disposición que se contraponga a lo estipulado en esta Resolución Exenta.

5. **DÉJESE ESTABLECIDO,** que la presente Resolución Exenta no afecta el presupuesto del Servicio.

ANÓTESE, NOTIFÍQUESE, CÚMPLASE Y ARCHÍVESE.

JUANA MYRIAM NAZAL BUSTOS
Firmado digitalmente por JUANA MYRIAM NAZAL BUSTOS
Fecha: 2020.11.19 13:50:19 -03'00'

JUANA NAZAL BUSTOS
DIRECTORA
SERVIU METROPOLITANO

Alejandra Hermosilla Hurtado

NURYS RAMÍREZ TAPIA
Ministro de Fe

AHH/DMB/EMA
DISTRIBUCIÓN:
- Subdirección de Administración y Finanzas.
- Subdirección de Pavimentación y Obras Viales.
- Subdirección de Vivienda y Equipamiento.
- Subdirección de Operaciones Habitacionales.
- Subdirección Jurídica.
- Departamento Administrativo.
- Departamento Servicios Generales
- Contraloría Interna SERVIU Metropolitano.
- Sección Secretaría General / Ministro de Fe SERVIU Metropolitano.
- Sección Informática
- Sección Gestión y Calidad.
- Sección Partes y Archivo.
- Sección Control de Gestión SDAF.

NO AFECTA PRESUPUESTO
M.Trinidad Diaz V.
09 NOVIEMBRE 2020
Subdepartamento de Presupuesto
Subdirección de Adm. Y Finanzas