# SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

## NCH-ISO 27001

---

## *POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL MINISTERIO DE VIVIENDA Y URBANISMO, PARA SU APLICACIÓN EN SERVIU METROPOLITANO*

---

Departamento Programación Física y Control
Sistema de Seguridad de la Información
OFPA N° 063

APRUEBA INTEGRACIÓN DE LA VERSIÓN N° 10 DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL MINISTERIO DE VIVIENDA Y URBANISMO, PARA SU APLICACIÓN EN SERVIU METROPOLITANO, Y DEJA SIN EFECTO ANTERIORES VERSIONES RELACIONADAS CON ESTA MATERIA.

**CON ESTA FECHA SE HA DICTADO LA SIGUIENTE:**

**RESOLUCIÓN EXENTA Nº** 1964 12/06/2025

**SANTIAGO,**

**VISTOS:**

**a.** La Ley Nº 18.575 de 1986, Orgánica Constitucional de Bases Generales de la Administración del Estado;

**b.** La Ley Nº 21.180 sobre Transformación Digital del Estado, promulgada con fecha 25 de octubre de 2019 y publicada con fecha el 11 de noviembre de 2019, que modifica las bases de los procedimientos administrativos para avanzar en su digitalización, contribuyendo así a la entrega de servicios más cercanos, simples y oportunos a la ciudadanía;

**c.** La Ley Nº 21.459 de fecha 20 de junio de 2022, del Ministerio de Justicia y Derechos Humanos, que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest;

**d.** La Ley Nº 21.663 de fecha 8 de abril de 2024, del Ministerio del Interior y Seguridad Pública, que establece la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información en Chile;

**e.** 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;

**f.** El Decreto Supremo Nº 83 de fecha 03 de junio 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;

**g.** El Decreto Supremo Nº 14 de fecha 15 de enero de 2014, del Ministerio de Economía, Fomento y Turismo, que modifica Decreto Nº 181/2002, que aprueba reglamento de la Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los Decretos que indica;

**h.** El Decreto Nº 83 de fecha 27 de abril de 2017, del Ministerio de Relaciones Exteriores, que promulga el Convenio sobre la Ciberdelincuencia;

**i.** El Decreto Nº 273 de fecha 13 de septiembre de 2022, del Ministerio del Interior y Seguridad Pública, que establece la obligación de Reportar Incidentes de Ciberseguridad;

**j.** El Decreto Nº 7 de fecha 17 de agosto de 2023, del Ministerio Secretaría General de la República, que establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N° 21.180;

**k.** El Decreto Nº 164 de fecha 04 de diciembre de 2023, del Ministerio del Interior y Seguridad Pública, que Aprueba la Política Nacional de Ciberseguridad 2023-2028, que contiene los lineamientos políticos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2028, para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente;

**l.** 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;

**m.** El Instructivo Presidencial Nº 001 de fecha 24 de enero de 2019, que imparte instrucciones sobre Transformación Digital en los órganos de la Administración del Estado;

**n.** La Norma NCh-ISO 27001 de Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información – Requisitos;

**o.** La Resolución Exenta Nº 5225 de fecha 29 de diciembre de 2023, de SERVIU Metropolitano, que aprueba integración de la versión N° 09 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;

**p.** La Resolución Exenta Nº 325, de fecha 04 de marzo de 2025, del Ministerio de Vivienda y Urbanismo que deja sin efecto Resolución Exenta Nº 1508, (V. y U.), de 2023, que aprueba la Política General de Seguridad de la Información, en su versión Nº 10, para el Ministerio de Vivienda y Urbanismo, sus Servicios de Vivienda y Urbanización, el Parque Metropolitano de Santiago y la Subsecretaría de Vivienda y Urbanismo (Nivel Central y sus Secretarias Ministeriales);

**q.** La Resolución N° 36 y 8, de fechas 19 de diciembre de 2024 y 24 de marzo de 2025 respectivamente, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón, de las materias que se indican;

**r.** El Decreto Exento RA N° 272/84/2023 (V. y U.) de fecha 01 de diciembre de 2023, que me nombra Director del Servicio de Vivienda y Urbanización Metropolitano, y las facultades que en tal carácter me competen en conformidad al D.S N° 355 (V. y U.) del año 1976, Reglamento Orgánico de los SERVIU, dicto la siguiente:

**CONSIDERANDO:**

**a.** Que, el surgimiento de nueva normativa legal que establece un marco en materia de Ciberseguridad e Infraestructura Crítica de la Información, se han dictado una serie de normas, entre las que se encuentran aquellas singularizadas en los Vistos de las letras b), c), d), f), g), h), i), j), k), l), m) y n) de la presente Resolución Exenta a aprobación;

**b.** Que, en conformidad a lo dispuesto en el numeral 6.4 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo, aprobada por medio de la Resolución Exenta N° 325, (V. y U.) de 2025, indica que: La presente política será revisada al menos una vez al año o cuando el/la Encargado/a de Seguridad de la Información y Ciberseguridad de uno o más Servicios lo requiera, para asegurar su continuidad e idoneidad, considerando los resultados de revisiones y auditorías realizadas, y los cambios que puedan producirse, tales como:

- Nuevas definiciones estratégicas, cambios en la institución y/o enfoques a la gestión de seguridad.
- Incorporación y/o modificaciones relevantes de procesos o actividades críticas de la institución.
- Cambios significativos al soporte tecnológico.
- Cambios significativos en los niveles de riesgo a que se expone la información.
- Modificación y/o creación de leyes o reglamentos que afecten la institución.
- Recomendaciones realizadas por autoridades pertinentes.
- Tendencias relacionadas con amenazas y vulnerabilidades.

**c.** Que es necesario, la integración de la versión Nº 10 de la Política General de Seguridad de la Información y Ciberseguridad del Ministerio de Vivienda y Urbanismo, para ser implementada en los Servicios de Vivienda y Urbanización, el Parque Metropolitano de Santiago y la Subsecretaría de Vivienda y Urbanismo (Nivel Central y sus Secretarias Ministeriales).

**APRUEBA INTEGRACIÓN DE LA VERSIÓN N° 10 DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL MINISTERIO DE VIVIENDA Y URBANISMO, PARA SU APLICACIÓN EN SERVIU METROPOLITANO, Y DEJA SIN EFECTO ANTERIORES VERSIONES RELACIONADAS CON ESTA MATERIA.**

**RESOLUCIÓN:**

I. **DÉJESE SIN EFECTO,** a partir de la total tramitación del presente acto administrativo, la Resolución Exenta Nº 5225 de fecha 29 de diciembre de 2023 del SERVIU Metropolitano, señalado en el visto o), que aprueba integración de la versión Nº 09 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo en SERVIU Metropolitano;

II. **APRUÉBASE,** la presente Resolución Exenta que Integra la versión Nº 10 de la Política General de Seguridad de la Información y Ciberseguridad del Ministerio de Vivienda y Urbanismo, aprobada por medio de la Resolución Exenta N° 325, (V. y U.) de 2025, para su aplicación en SERVIU Metropolitano, a partir de la fecha de tramitación de la presente Resolución:

# POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

## *SERVICIO DE VIVIENDA Y URBANIZACIÓN*

### 1. OBJETIVO:

- Proteger los activos físicos y digitales de SERVIU Metropolitano, preservando los principios de confidencialidad, integridad y disponibilidad de la información. Identificar oportunamente los riesgos asociados a los productos estratégicos (bienes y/o servicios) establecidos en las definiciones estratégicas institucionales (Formulario A1) para asegurar la continuidad operacional.

### 2. ALCANCE:

- Es aplicable al personal del Servicio, incluyendo aquellos con calidad jurídica de Planta, Contrata y Honorarios, así como a las personas que cumplen funciones específicas en el Servicio, tales como Asesores, Consultores y Practicantes. En resumen, abarca a todas las personas que trabajan o colaboran en SERVIU Metropolitano, independientemente de la modalidad de trabajo que realicen, ya sea presencial, a distancia, teletrabajo u otra, conforme a las condiciones establecidas por la legislación vigente.

- Además, incluye a las empresas que prestan servicios a este organismo y que, para su desempeño, utilizan y acceden a todo tipo de información y a los productos estratégicos (bienes y/o servicios) establecidos en las definiciones estratégicas institucionales (Formulario A1).

### 3. ROLES Y RESPONSABILIDADES:

- A continuación, se detalla el esquema relacional de la Estructura funcional para la implementación y mantenimiento del Sistema de Seguridad de la Información y Ciberseguridad,[1] con la Identificación de sus miembros y sus responsabilidades, y que tienen un papel fundamental en la coordinación de decisiones, supervisión, desarrollo e implementación, en conformidad a la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo integrado en SERVIU Metropolitano.

[1] Resol. Ex. de Roles y Responsabilidades de la Estructura Funcional del Comité de Seguridad de la Información y Ciberseguridad, aprobada y difundida en SERVIU Metropolitano.

### 3.1 DIRECTOR/A DEL SERVIU METROPOLITANO:

- Responsable de la supervisión general del Sistema de Seguridad de la Información y Ciberseguridad en SERVIU Metropolitano.


### 3.2 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN:

- Es el órgano de participación interna del Servicio responsable/encargado de asesorar en la implementación de procedimientos estándares que se desprenden de las Políticas en materia de Seguridad de la Información y Ciberseguridad en SERVIU Metropolitano.

- Está integrado por: el(la) Encargado/a de Seguridad de la Información y Ciberseguridad, el(la) Coordinador/a de Seguridad de la Información y Ciberseguridad, y las Jefaturas de la Subdirección de Vivienda y Equipamiento, Subdirección de Pavimentación y Obras Viales, Subdirección de Operaciones Habitacionales, Departamento Gestión Inmobiliaria, Subdirección Jurídica, Subdirección de Administración y Finanzas, Departamento Programación Física y Control, Contraloria Interna y Sección Comunicaciones.


### 3.3 EQUIPO TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN:

- Conformado por el(la) Encargado/a Técnico de Seguridad de la Información y Ciberseguridad, y las Contrapartes en Seguridad de la Información y Ciberseguridad: Encargado/a Sección Gestion de Procesos, Encargada/o Gestión de las Personas para la Seguridad de la Información, Encargado/a de Activos de Información Digitales, Encargado/a de Activos de Información Físicos, Encargado/a de Infraestructura para la Seguridad de la Información, Encargada/o de Reportes y Registros Incidentes para la Seguridad de la Información.

- A continuación, se detalla la estructura funcional del Equipo Técnico de Seguridad de la Información y Ciberseguridad, con sus roles y funciones, con el objeto de gestionar, establecer, implementar, mantener y mejorar continuamente la Documentación de Seguridad de la Información:


## 4. DEFINICIONES:

- SERVIU Metropolitano reconoce el valor de la información como un activo fundamental de la organización, que debe ser debidamente protegido. Para ello, se enfoca en minimizar los riesgos y asegurar la continuidad operacional de sus funciones, implementando controles indispensables durante el año t. Estos controles garantizan que los activos físicos y digitales estén disponibles para el personal del Servicio y las personas que realizan funciones específicas en la Institución. Además, se verifica regularmente el cumplimiento de estos controles mediante prácticas de seguridad y mecanismos que aseguran la integridad de la información almacenada en equipos, sistemas e infraestructura.

- Los controles de la Norma NCh-ISO 27001 implementados en SERVIU Metropolitano son:

| SISTEMA DE SEGURIDAD DE LA INFORMACIÓN Norma NCh-ISO 27001 | | |
|---|---|---|
| N° | Controles ISO 27001 | Objetivo del Control |
| 1 | A.5.1.1 | Políticas para la Seguridad de la Información. |
| 2 | A.5.1.2 | Revisión de las Políticas de Seguridad de la Información. |
| 3 | A.6.1.1 | Roles y responsabilidades de la Seguridad de la Información. |
| 4 | A.6.1.2 | Segregación de funciones. |
| 5 | A.6.1.3 | Contacto con autoridades. |
| 6 | A.6.2.1 | Política de dispositivos móviles. |
| 7 | A.7.1.1 | Selección. |
| 8 | A.7.2.1 | Responsabilidades de la dirección. |
| 9 | A.7.2.2 | Toma de conciencia, educación y formación en seguridad de la información. |
| 10 | A.7.2.3 | Proceso disciplinario. |
| 11 | A.7.3.1 | Responsabilidades en la desvinculación o cambio de empleo. |
| 12 | A.8.1.1 | Inventario de activos. |
| 13 | A.8.1.4 | Devolución de activos. |
| 14 | A.8.3.1 | Gestión de los medios Removibles. |
| 15 | A.8.3.2 | Eliminación de los medios. |
| 16 | A.8.3.3 | Transferencia física de los medios. |
| 17 | A.9.1.1 | Política de control de acceso. |
| 18 | A.9.1.2 | Acceso a las redes y a los servicios de la red. |
| 19 | A.11.1.1 | Perímetro de seguridad física. |
| 20 | A.11.2.1 | Ubicación y protección del equipamiento. |
| 21 | A.11.2.4 | Mantenimiento del equipamiento. |

| N° | Controles ISO 27001 | Objetivo del Control |
|---|---|---|
| 22 | A.11.2.7 | Seguridad en la reutilización o descarte de equipos. |
| 23 | A.11.2.8 | Equipo de usuario desatendido. |
| 24 | A.11.2.9 | Política de escritorio y pantalla Límpios. |
| 25 | A.12.2.1 | Controles contra código malicioso. |
| 26 | A.12.3.1 | Respaldo de la Información. |
| 27 | A.12.4.1 | Registro de eventos. |
| 28 | A.12.6.2 | Restricciones sobre la instalación de software. |
| 29 | A.15.1.1 | Política de seguridad de la información para las relaciones con el proveedor. |
| 30 | A.15.2.1 | Supervisión y revisión de los servicios del proveedor. |
| 31 | A.16.1.1 | Responsabilidades y Procedimientos. |
| 32 | A.16.1.2 | Informe de Eventos de Seguridad de la Información. |
| 33 | A.16.1.5 | Respuesta ante Incidentes de Seguridad de la Información. |
| 34 | A.17.1.1 | Planificación de la continuidad de la seguridad de la información. |
| 35 | A.18.1.3 | Protección de los Registros. |
| 36 | A.18.1.4 | Privacidad y Protección de la Información de Identificación personal. |
| 37 | A.18.2.1 | 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 y sus políticas específicas, procedimientos y normativas que integran el Sistema de Seguridad de la Información y Ciberseguridad, deberá efectuarse, al menos una vez al año por el Comité de Seguridad de la Información y Ciberseguridad, 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. De no existir cambios significativos en el Servicio las reuniones semestrales del Comité de seguridad de la Información y Ciberseguridad serán consideradas proceso de revisión por la Dirección.

- La formalización, modificación y actualización del presente documento, así como toda la documentación vinculada al Sistema de Seguridad de la Información y Ciberseguridad, 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 y Ciberseguridad, será comunicada a través de los canales de difusión establecidos, pudiendo ser por correo electrónico, publicación en la INTRANET, u otro medio que la Institución considere pertinente, asegurando que el contenido de la documentación sea accesible y comprensible para todo el personal del SERVIU Metropolitano.

- Cada vez que SERVIU Metropolitano realice un proceso de contratación de servicio con alguna Empresa Proveedora, 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.

- Adicionalmente, la Política General como las Políticas Específicas de Seguridad de la Información y Ciberseguridad se encuentran publicadas en la página web institucional, disponible para consulta permanente del funcionariado o personal externo que prestan servicios para el SERVIU Metropolitano, por lo que se entenderá conocido por todos.

## 7. SANCIONES APLICABLES:

- El presente documento tiene su base en las definiciones, términos y controles descritos en la Norma Chilena NCh-ISO 27001 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 la presente Política y toda documentación vinculada al Sistema de Seguridad de la Información y Ciberseguridad, debidamente acreditado, conllevará a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los(as) 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 y Ciberseguridad, 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 con 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 el(la) Encargado/a de la Seguridad de la Información y Ciberseguridad y enviará al Comité de Seguridad de la Información y Ciberseguridad del Servicio, para la toma de conocimiento.

## 9. DOCUMENTOS RELACIONADOS:

- Ley Nº 21.180 sobre Transformación Digital del Estado, publicada el 11 de noviembre de 2019, modifica las bases de los procedimientos administrativos para avanzar en su digitalización, contribuyendo así a la entrega de servicios más cercanos, simples y oportunos a la ciudadanía.
- Ley Nº 21.459 de fecha 20 de junio de 2022, del Ministerio de Justicia y Derechos Humanos, que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
- Ley Nº 21.663 de fecha 8 de abril de 2024, del Ministerio del Interior y Seguridad Pública, que establece que establece la Ley de Marco de Ciberseguridad e Infraestructura Crítica de la Información en Chile.
- Decreto Supremo Nº 83 de fecha 03 de junio 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.
- Decreto Supremo Nº 14 de fecha 15 de enero de 2014, del Ministerio de Economía, Fomento y Turismo, que modifica Decreto Nº 181/2002, que aprueba reglamento de la Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los Decretos que indica.

- Decreto Nº 83 de fecha 27 de abril de 2017, del Ministerio de Relaciones Exteriores, que promulga el Convenio sobre la Ciberdelincuencia.
- Decreto Nº 273 de fecha 13 de septiembre de 2022, del Ministerio del Interior y Seguridad Pública, que establece la obligación de Reportar Incidentes de Ciberseguridad.
- Decreto Nº 7 del año 2023, del Ministerio Secretaría General de la República, que Establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N° 21.180.
- Decreto Nº 164 del 04 de diciembre del 2023, del Ministerio del Interior y Seguridad Pública, que Aprueba la Política Nacional de Ciberseguridad 2023-2028, que contiene los lineamientos políticos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2028, para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente.
- 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.
- Instructivo Presidencial Nº 001 de fecha 24 de enero de 2019, que imparte instrucciones sobre Transformación Digital en los órganos de la Administración del Estado.
- Norma NCh-ISO 27001 de Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.
- Resolución Exenta que aprueba integración de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo, para su aplicación en SERVIU Metropolitano.
- Resolución de Roles y Responsabilidades de la Estructura Funcional del Comité de Seguridad de la Información y Ciberseguridad, para su aplicación en SERVIU Metropolitano.

## 10. CONTROL DE VERSIONES:

| N° Resol Ex | Fecha | Principales puntos modificados |
|---|---|---|
| 1831 | 24.03.2011 | Se adopta la Política de Seguridad del Ministerio de Vivienda y Urbanismo en el SERVIU Metropolitano, disposición que ha sido observada por Analista de Red de Expertos de la Dirección de Presupuestos del Ministerio de Hacienda. Dicho acto constituye, además, el Comité de Gestión de Seguridad y Confidencialidad de la Información. |
| 6800 | 30.11.2011 | Modifica Política General de Seguridad de la Información para SERVIU Metropolitano y deja sin efecto adopción de Política de Seguridad del MINVU según Resolución Exenta Nº 1831 de 2011. |
| 7101 | 27.12.2013 | Aprueba nueva versión de Política General de Seguridad de la Información para SERVIU RM y deja sin efectos anteriores versiones relacionados con esta materia. |
| 7661 | 21.12.2015 | Aprueba Integración de la versión Nº 05 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo con Resolución Exenta Nº 9103 de fecha 23 de noviembre de 2015, y deja sin efecto anteriores versiones relacionadas con esta materia. |
| 6601 | 28.11.2017 | Aprueba Integración de la versión Nº 06 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo con Resolución Exenta Nº 13.543 de fecha 17 de noviembre de 2017, y deja sin efecto anteriores versiones relacionadas con esta materia. |
| 4675 | 27.09.2019 | Aprueba Integración de la versión Nº 08 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo con Resolución Exenta Nº 2097 de fecha 12 de septiembre del 2019, y deja sin efecto anteriores versiones relacionadas con esta materia. |
| 5225 | 29.12.2023 | Aprueba Integración de la versión Nº 09 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo con Resolución Exenta Nº 1508 de fecha 08 de septiembre del 2023, y deja sin efecto anteriores versiones relacionadas con esta materia. |

III. **ESTABLÉCESE,** que la presente Resolución Exenta, que integra la versión Nº 10 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo, será almacenada en el sitio del Sistema de Seguridad de la Información ubicado en la INTRANET del Servicio y, difundido al funcionariado a través de mecanismos de la comunicación interna existentes en SERVIU Metropolitano.

IV. **ESTABLÉCESE,** la obligación del Encargado/a de Seguridad de la Información y Ciberseguridad, en coordinación con el Comité de Seguridad de la Información del SERVIU Metropolitano, de velar y garantizar el estricto cumplimiento de la integración de esta política, ratificada por la presente Resolución Exenta.

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

VI. **DÉJESE** constancia, que la presente Resolución no afecta el presupuesto del Servicio.

**ANÓTESE, NOTIFÍQUESE Y CÚMPLASE**

SERVICIO DE VIVIENDA Y URBANIZACIÓN DIRECTOR REGIÓN METROPOLITANA

**ROBERTO ACOSTA KERUM**
**DIRECTOR**
**SERVIU METROPOLITANO**

SERVICIO DE VIVIENDA Y URBANIZACIÓN MINISTRO DE FE

NURYS RAMIREZ TAPIA
Ministro de Fe

NO AFECTA PRESUPUESTO
Karen Valdivia Rojas
29 MAYO 2025
Subdepartamento de Presupuesto
Subdirección de Adm. y Finanzas

**JES/FBC/MLM/RAA/GSV/RRA/CRS/EMA/**

**TRANSCRIPCIÓN:**

1. Subdirección de Administración y Finanzas.
2. Subdirección de Vivienda y Equipamiento.
3. Subdirección de Operaciones Habitacionales.
4. Subdirección de Pavimentación y Obras Viales.
5. Subdirección Jurídica.
6. Departamento Programación Física y Control.
7. Departamento Gestión Inmobiliaria.
8. Contraloría Interna SERVIU Metropolitano.
9. Ministro de Fe.
10. Sección Partes y Archivo.
11. Sección Gestión de Procesos.

Ministerio de Vivienda y Urbanismo

Gobierno de Chile

**MODIFIQUESE LA RESOLUCIÓN EXENTA N°1508, (V. y U.), DE 2023, QUE APRUEBA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO, SUS SERVICIOS DE VIVIENDA Y URBANIZACIÓN, EL PARQUE METROPOLITANO DE SANTIAGO Y LA SUBSECRETARÍA DE VIVIENDA Y URBANISMO (NIVEL CENTRAL Y SUS SECRETARIAS REGIONALES MINISTERIALES).**

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA
04 MAR 2025
RESOLUCIÓN EXENTA
TRAMITADA

**SANTIAGO,** 04 MAR. 2025 HOY SE RESOLVIÓ LO QUE SIGUE

**RESOLUCIÓN EXENTA N°** Nº. 325

**VISTOS:** Lo dispuesto en la Ley N° 16.391, que crea el Ministerio de la Vivienda y Urbanismo; el D.L. N°1305 de 1975 que reestructura y regionaliza el Ministerio de Vivienda y Urbanismo; en el D.S. N°83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado sobre la Seguridad y Confidencialidad de los documentos electrónicos; D.S. N°181, de 2012, del Ministerio de Economía, Fomento y Turismo, que aprueba reglamento de la Ley N°19.799 sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha firma; el D.S. N°164 de 2023 que aprobó la Política Nacional de Ciberseguridad 2023-2028; el Instructivo Presidencial N°8 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; el D.S. N°273 de 2022, del Ministerio del Interior y Seguridad Pública, que establece la obligación de reportar incidentes de ciberseguridad; el D.S. N°7, de 2023, del Ministerio Secretaría General de la Presidencia, que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la ley N°21.180; la Resolución Exenta N°1.508 (V. y U.), de 2023, que aprueba la Política General de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo; la Resolución N°1.238, (V. y U.), de 2023 que actualiza la estructura funcional para el Sistema de Seguridad de la Información y Ciberseguridad; la Ley N°21.663, Ley Marco de Ciberseguridad; y 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, el surgimiento de nueva normativa legal, como la Ley N°21.663, que establece un marco en materia de Ciberseguridad e Infraestructura Crítica de la Información; la actualización de los marcos referentes (como la nueva versión de la ISO 27001:2022, NIST CSF 2.0), y la confección de estándares sectoriales relevantes (como la RAN 20-10) generan un desafío constante en los distintos organismos y servicios públicos y sus equipos de seguridad de la información actualizar sus herramientas y metodologías para evaluar o incorporar las nuevas exigencias en sus normativas y regulaciones internas.

**b)** Que, sumado a lo indicado en el considerando anterior, el marco normativo de la Seguridad de la Información y Ciberseguridad, también considera una serie de normas como 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; D.S N°181, de 2002, de Ministerio de Economía, Fomento y Turismo, que aprueba reglamento de la Ley N°19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; el Instructivo Presidencial N°8 de 2018 que imparte instrucciones en materias de Ciberseguridad a los órganos de la administración del Estado la Política Nacional de Ciberseguridad de 2023; el D.S. N°164 de 2023 que aprobó la Política Nacional de Ciberseguridad 2023-2028; el D.S. N°7, de 2023, del Ministerio del Interior y Seguridad Pública, que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme lo establecido en la Ley N°21.180, entre otras.

**c)** Que, en conformidad a lo dispuesto en el numeral 6.4 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo, aprobada por medio de la Resolución Exenta N°1508, (V. y U.), de 2023, indica que: *"La presente política será revisada al menos una vez al año o cuando el/la Encargado/a de Seguridad de la Información y Ciberseguridad de uno o más Servicios lo requiera, para asegurar su continuidad e idoneidad, considerando los resultados de revisiones y auditorías realizadas, y los cambios que puedan producirse, tales como:*

- *Nuevas definiciones estratégicas, cambios en la institución y/o enfoques a la gestión de seguridad.*
- *Incorporación y/o modificaciones relevantes de procesos o actividades críticas de la institución.*
- *Cambios significativos al soporte tecnológico.*
- *Cambios significativos en los niveles de riesgo a que se expone la información.*
- *Modificación y/o creación de leyes o reglamentos que afecten la institución.*
- *Recomendaciones realizadas por autoridades pertinentes.*

- *Tendencias relacionadas con amenazas y vulnerabilidades".*

**d)** Que, en mérito de lo anterior dicto la siguiente:

**RESOLUCIÓN:**

**1.- MODIFÍQUESE** la Resolución Exenta N°1508, (V. y U.), de 08 de septiembre de 2023, referida en los considerandos de esta resolución, en el sentido de reemplazar todos sus considerandos por los siguientes:

***a)*** *Que, el surgimiento de nueva normativa legal, como la Ley N°21.663, que establece un marco en materia de Ciberseguridad e Infraestructura Crítica de la Información, pero que aún no se encuentra vigente; la actualización de los marcos referentes (como la nueva versión de la ISO 27001:2022, NIST CSF 2.0), y la confección de estándares sectoriales relevantes (como la RAN 20-10) generan un desafío constante en los distintos organismos y servicios públicos y sus equipos de seguridad de actualizar sus herramientas y metodologías para evaluar o incorporar las nuevas exigencias en sus normativas y regulaciones internas.*

***b)*** *Que, sumado a lo indicado en el considerando anterior, el marco normativo de la Seguridad de la Información y Ciberseguridad, también considera una serie de normas como 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; D.S N°181, de 2002, de Ministerio de Economía, Fomento y Turismo, que aprueba reglamento de la Ley N°19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; el Instructivo Presidencial N°8 de 2018 que imparte instrucciones en materias de Ciberseguridad a los Órganos de la Administración del Estado la Política Nacional de Ciberseguridad de 2023; el D.S. N°164 de 2023 que aprobó la Política Nacional de Ciberseguridad 2023-2028; el D.S. N°7, de 2023, del Ministerio del Interior y Seguridad Pública, que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme lo establecido en la Ley N°21.180, entre otras.*

***c)*** *Que, en conformidad a lo dispuesto en el numeral 6.4 de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo, aprobada por medio de la Resolución Exenta N°1508, (V. y U.), de 2023, indica que: "La presente política será revisada al menos una vez al año o cuando el/la Encargado/a de Seguridad de la Información y Ciberseguridad de uno o más Servicios lo requiera, para asegurar su continuidad e idoneidad, considerando los resultados de revisiones y auditorías realizadas, y los cambios que puedan producirse, tales como:*

- *Nuevas definiciones estratégicas, cambios en la institución y/o enfoques a la gestión de seguridad.*

- *Incorporación y/o modificaciones relevantes de procesos o actividades críticas de la institución.*
- *Cambios significativos al soporte tecnológico.*
- *Cambios significativos en los niveles de riesgo a que se expone la información.*
- *Modificación y/o creación de leyes o reglamentos que afecten la institución.*
- *Recomendaciones realizadas por autoridades pertinentes.*
- *Tendencias relacionadas con amenazas y vulnerabilidades.*

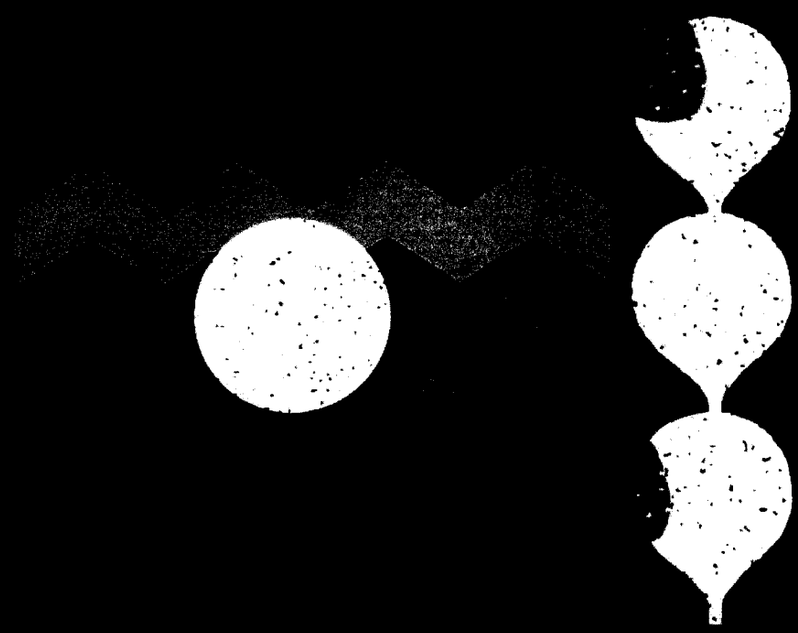
**d)** *Que, en mérito de lo anterior dicto la siguiente:*

**2.- MODIFÍQUESE** la Resolución Exenta N°1508, (V. y U.), de 08 de septiembre de 2023, en su parte resolutiva, en el sentido de reemplazar su resuelvo II por el siguiente:

***II.- APRUEBESE*** *la Política General de Seguridad de la Información y Ciberseguridad del Ministerio de Vivienda y Urbanismo, que rige a la Subsecretaría de Vivienda y Urbanismo, las Secretarías Regionales Ministeriales de Vivienda y Urbanismo; los Servicios de Vivienda y Urbanización y el Parque Metropolitano de Santiago, que se detalla a continuación:*

# Política de Seguridad de la Información y Ciberseguridad

Ministerio de Vivienda y Urbanismo



Ministerio de Vivienda y Urbanismo

Gobierno de Chile

## CONTENIDO



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

# 0. GLOSARIO

| | |
|---|---|
| **Activo** | ***Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio, sea a otras instituciones de la Administración del Estado o con personas naturales o jurídicas.*** |
| **Activo de Información** | ***Datos o información cuyo tratamiento es esencial para el desarrollo de las funciones propias de la institución que lo utiliza, genera, almacena, envía o intercambia, y que deben ser protegidos en su confidencialidad, integridad, disponibilidad u otros factores de importancia. Los activos de información pueden tener formato físico, electrónico o verbal, ser equipos o aplicativos, o incluso las personas cuyo conocimiento sirve para lograr los propósitos u objetivos de la Institución.*** |
| **Ciberseguridad y Seguridad de la Información** | ***Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de los órganos de la Administración del Estado, aumentando su resiliencia en el tiempo.*** |
| **Confidencialidad** | Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. |
| **Control de Seguridad** | ***Conjunto de estándares, buenas prácticas y normativas que permiten administrar los riesgos en las tecnologías de la información.*** |
| **Disponibilidad** | Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad o proceso autorizada. |
| **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.*** |
| **Gestión de Riesgo** | ***Proceso estructurado y proactivo por el cual se identifican, evalúan, controlan y tratan los riesgos derivados de una o más amenazas determinadas.*** |
| **Incidente de Seguridad de la Información** | ***Todo evento de seguridad o una serie de ellos, de carácter no deseado o inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos*** |

| | |
|---|---|
| | ***y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan comprometer las operaciones del negocio, la continuidad del servicio 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** | ***Propiedad de mantener la información con exactitud, autenticidad y completitud.*** |
| **Plataforma electrónica (en adelante también "plataforma")** | ***Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.*** |
| **Riesgo** | ***Efecto de la incertidumbre sobre los activos de información y los objetivos de una entidad, habitualmente expresado en relación con las consecuencias de un evento o incidente de seguridad y su probabilidad de ocurrencia.*** |
| **Seguridad de la Información** | Preservación de la confidencialidad, integridad y disponibilidad de la información. |
| **Servidor** | ***Equipo virtual o físico dedicado a entregar servicios de red, servicios de bases de datos, sitios web, sistemas informáticos, carpetas compartidas y, en general, brindar los recursos necesarios para responder las peticiones de usuarios.*** |
| **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. |
| ***Usuarios(as)*** | ***Funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo empresas que presten servicios en el Ministerio de Vivienda y Urbanismo, en la Subsecretaría de Vivienda y Urbanismo, en las Secretarias Regionales Ministeriales, en los Servicios de Vivienda y Urbanismo y el Parque Metropolitano de Santiago.*** |

# 1. DECLARACIÓN INSTITUCIONAL

El Ministerio de Vivienda y Urbanismo -MINVU- se ha comprometido a establecer, mantener y mejorar continuamente un Sistema de Seguridad de la Información ***y Ciberseguridad***-en adelante el SSI-, ***y un modelo de Gobernanza de Datos***, siendo éste un *"compromiso en el fomento y desarrollo de una cultura de la seguridad, basado en preservar los principios de confidencialidad, integridad y disponibilidad de la información, en beneficio de la ciudadanía y partes interesadas para alcanzar los objetivos institucionales, contribuyendo al fortalecimiento del Derecho a la Ciudad y a una Vivienda Digna y Adecuada, con enfoque territorial y perspectiva de género, poniendo énfasis en la ejecución del Plan de Emergencia Habitacional, el Mejoramiento de Viviendas y Entornos para vivir en Comunidad, la Construcción de Ciudades Justas para el encuentro ciudadano, la recuperación de suelo e inmuebles para las familias y la Modernización de la gestión".*

Por tal motivo la información es un activo esencial para que el MINVU avance hacia el cumplimiento de su misión ministerial, entendiendo por Activo de Información, todos aquellos elementos que hacen posible o sustentan los procesos operacionales, como las personas que utilizan la información; los equipos, sistemas e infraestructura que soporta la información; ***los datos que se generan;*** y la información propiamente tal en cualquiera de sus múltiples formatos.

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[1].

# 2. OBJETIVO GENERAL

El objetivo de este documento es:

- Establecer los lineamientos institucionales y entregar orientación en ***materias de*** Seguridad de la Información ***y Ciberseguridad y Gobernanza de Datos dentro*** del Ministerio de Vivienda y Urbanismo.
- Definir los objetivos y principios para guiar las actividades relacionadas con la seguridad de la información ***y la gobernanza de datos***, con el fin de contar con información precisa, completa, y disponible de manera oportuna y así permitir el logro de los objetivos institucionales, la eficiencia de los procesos y el cumplimiento de la legislación.

## 2.1 Objetivos específicos de la Seguridad de la Información, *Ciberseguridad y Gobernanza de Datos*

El Sistema de Seguridad de la Información del MINVU **y el Modelo de Gobernanza de Datos** se alinean y permiten soportar los objetivos estratégicos ministeriales definidos en la Ficha de Definiciones Estratégicas A0[2]. La institución establece los siguientes objetivos de la gestión de seguridad de la información:

- Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la Seguridad de la Información.

---

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

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

A0[2]. La institución establece los siguientes objetivos de la gestión de seguridad de la información:

- Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la Seguridad de la Información.
- Establecer los niveles de acceso apropiados a la información, brindando y asegurando la ***preservación de la*** confidencialidad, integridad y disponibilidad que requiera cada sistema, proceso, actividad crítica y usuario.
- Apoyar el modelo ***y/o procesos referente*** a las gestiones tendiente a asegurar la continuidad de negocio, a través de acciones tendientes a gestionar los incidentes y a revertir y resolver contingencias que se detecten.
- Establecer un marco de Gestión de Riesgo Cibernético para cada sistema, proceso, actividad crítica, que permita alcanzar los objetivos estratégicos.

Para lo anterior, en el marco del SSI, se establecen un conjunto de controles aplicables, seleccionados a través de un proceso de gestión de riesgos y la formalización de políticas, procesos, procedimientos para proteger los activos de información en consistencia con los principios establecidos en el punto 5 de esta política.

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

La presente política es aplicable a todos los procesos[3] vinculados a los objetivos ministeriales y productos estratégicos del MINVU.

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, de la Subsecretaría de Vivienda y Urbanismo, las Secretarias Regionales Ministeriales, así como de los servicios que se relacionan con esta Secretaría de Estado, es decir, los Servicios de Vivienda y Urbanización y el Parque Metropolitano de Santiago, incluyendo a asesores, consultores, practicantes y personas naturales o jurídicas, que se relacionen o que se encuentran vinculadas con el MINVU en virtud de contratos, convenios, normativa vigente, entre otros. En el caso de *"el personal"*, les aplica indistintamente de la modalidad de trabajo que realice, ya sea *"presencial"*, *"a distancia"*, *"teletrabajo"* u otra, en las condiciones que establezca la legislación vigente.

Para dar cumplimiento a los requisitos, el MINVU 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 puede definir las políticas específicas que considere necesarias y que sean de aplicación local; estos documentos no pueden contener elementos que contravengan la presente política, aplicándose además esta última en todos los aspectos no regulados por aquellas.

---

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

[3] Los procesos se encuentran definidos en el Mapa de Procesos Ministerial.

# 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**: cuyo rol asesora a la jefatura de cada Servicio en materias relativas a Seguridad de la Información y Ciberseguridad, coordinar las acciones tendientes a cumplir y apoyar los objetivos de seguridad de la información y lidera la identificación de amenazas o riesgos en la seguridad de la información o de sus instalaciones.
- **Comité de Seguridad de la Información** o Comité de similar denominación: formado por un equipo multidisciplinario de alto nivel en cada Servicio que tiene injerencia en las decisiones estratégicas relativas a la seguridad de la información, así como también en la supervisión y monitoreo del SSI.
- ***Encargado/a de Activos de Información, quien será el (la) responsable de su identificación y clasificación, así como gestionar el riesgo y niveles de seguridad asociados, en conformidad a lo dispuesto en el artículo 5° del Decreto Supremo N°7 de 2023, del Ministerio del Interior y Seguridad Pública.***

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. PRINCIPIOS PARA EL RESGUARDO DE 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 éstos.

A continuación, se describe cómo el MINVU aborda los 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[4] 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

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

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 de acuerdo con la legislación vigente, revisando periódicamente estos lineamientos ***y considerando el ciclo de vida de los activos de información.***

## 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 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 ***interrumpa*** la continuidad del flujo de información.

# 6. GESTIÓN DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN *Y CIBERSEGURIDAD*

## 6.1 Generación de una política y otros documentos

La Política de Seguridad de la Información ***y Ciberseguridad*** 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.

## 6.2 Aprobación de una política y otros documentos

La Política General y las Políticas Específicas de Seguridad son aprobadas a través de un acto administrativo suscrito por el Jefe de Servicio, facultad que no puede ser delegada.

***Los demás documentos que se requiera emitir,*** como normativas, procedimientos e instructivos son aprobados a través de un acto administrativo igualmente suscrito por el 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

con 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 deberá efectuar a través de los canales de difusión establecidos, pudiendo utilizarse publicación en el ***sitio "Sistema de Seguridad de la Información"*** y/o Minvuletín y/o Correo electrónico y/o Afiches y/o volantes, u otro medio que la institución considere pertinente ***para lograr la difusión del presente instrumento.***

Adicionalmente, tanto la política general como las políticas específicas de seguridad de la información ***de aplicación transversal a todos los Servicios dependientes del MINVU*** se encuentran publicadas en la página web institucional disponible para consulta de personal o terceras partes que prestan servicios para el MINVU y para la ciudadanía en general.

## 6.4 Revisión de la Política *de Seguridad de la Información y Ciberseguridad*

La presente política será revisada al menos una vez al año o cuando el/la ***Encargado/a de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos (o similar)*** de uno o más Servicios lo requiera, para asegurar su continuidad e idoneidad, considerando los resultados de revisiones y auditorías realizadas, y los cambios que puedan producirse, tales como:

- Nuevas definiciones estratégicas, cambios en la institución y/o enfoques a la gestión de seguridad.
- Incorporación y/o modificaciones relevantes de procesos o actividades críticas de la institución.
- Cambios significativos al soporte tecnológico.
- Cambios significativos en los niveles de riesgo a que se expone la información.
- Modificación y/o creación de leyes o reglamentos que afecten a la institución.
- Recomendaciones realizadas por autoridades pertinentes.
- Tendencias relacionadas con amenazas y vulnerabilidades.

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.

# 7. SANCIONES APLICABLES

El incumplimiento ***o infracción*** de esta Política de Seguridad de la Información ***y Ciberseguridad, por parte de los funcionarios del MINVU, SEREMI, SERVIU y PARQUEMET, acarrea responsabilidad administrativa, debiendo aplicarse alguna de las medidas disciplinarias previstas en el Estatuto Administrativo (censura, multa, suspensión o destitución),*** previa ***instrucción*** y sustanciación del respectivo ***Procedimiento Administrativo Disciplinario***; 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.

# 8. CONTROL DE VERSIONES

| Versión | Fecha Aprobación | Motivo de la revisión | Autor(es) |
|---|---|---|---|
| 09 | Julio 2023 | Revisión anual. Se identifican los cambios en negrita y cursiva. | Ivonne Valdivia / DIVAD; Marcela Jara/ DIFIN; Tomás Yanquez/DIFIN; Leonardo Cavieres/ DINFO; Claudio Paredes/ DINFO; Erick Atenas/ DINFO; M. Paula Melis Otonel/ Contralora Interna SERVIU Araucanía; Alexis Cornejo Marín/ Unidad de Informática SERVIU Atacama; Marcelo López Otárola/ Depto. Programación Física y Control SERVIU BioBío. |
| 10 | Enero 2025 | Revisión anual. Se incorporan aspectos del D.S. N°7, de 2023, del Ministerio Secretaría General de la Presidencia, que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N°21.180, y cambios de redacción. | Ivonne Valdivia / DIVAD; Litsi Contreras / DIJUR; Marcela Jara / DIFIN; Leonardo Cavieres / DINFO; Claudio Paredes / DINFO; Erick Atenas / DINFO; Gladys Martin / CIM; M. Paula Melis Otonel / Contralora Interna SERVIU Araucanía. |
| **Revisión:** | | | Carlos Araya Salazar/ Subsecretario de Vivienda y Urbanismo (S).<br>Vania Navarro Morales/ ***Encargada de Seguridad de la Información y Ciberseguridad y Gobernanza de Datos, Jefa División de Finanzas***<br>***Comité de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos Subsecretaría de V. y U.***<br>Encargados/as de Seguridad de la Información de SERVIU y Parque Metropolitano de Santiago. |
| **Aprobación:** | | | Carlos Montes Cisternas / Ministro de Vivienda y Urbanismo. |

**3.- MODIFÍQUESE** la Resolución Exenta N°1508, (V. y U.), de 08 de septiembre de 2023, referida en los considerandos de esta resolución, en el sentido de reemplazar su resuelvo III y IV por el siguiente:

***II.- INSTRUYASE*** *a las/os Encargadas/os de Seguridad de la Información y Ciberseguridad de la Subsecretaría de Vivienda y Urbanismo, de las Secretarías Regionales Ministeriales de Vivienda y Urbanismo, de los Servicios de Vivienda y Urbanización y del Parque Metropolitano de Santiago, de llevar acabo la difusión y sociabilización de la política fijada en este instrumento a todos los equipos de trabajo y funcionarios, así como de ejecutar todas las acciones tendientes a su implementación y velar por su estricto cumplimiento.*

***III.- DEJESE*** *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.*

**4.- MANTENGASE** en todo lo no modificado por esta resolución, la Resolución Exenta N°1508, (V. y U.), de 08 de septiembre de 2023.

**ANÓTESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.**

**CARLOS MONTES CISTERNAS**
**MINISTRO DE VIVIENDA Y URBANISMO**

**LO QUE TRANSCRIBO PARA SU CONOCIMIENTO**

**GABRIELA ELGUETA POBLETE**
**SUBSECRETARIA DE VIVIENDA Y URBANISMO**

CAS/CGB/MARC/DCC/PMG/VNM/MJC/

**DISTRIBUCION:**
- Gabinete Ministro V. y U.
- Gabinete Subsecretaria V. y U.
- SEREMI (16)
- Directores/as SERVIU (16)
- Director/a PARQUEMET
- Divisiones Nivel Central (7)
- Auditoría Interna Ministerial
- Contraloría Interna Ministerial
- Comisión Asesora para la Reducción de Riesgos de Desastres y Reconstrucción
- Sistema Integrado de Atención a la Ciudadanía (SIAC)
- Depto. Comunicaciones
- Centro de Estudios de Ciudad y Territorio (CECYT)
- Equipo de Estudios Económicos y de Procesos-DIFIN
- Sección Partes y Archivos

# SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

## NCH-ISO 27001

---

# *POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR, PARA SU APLICACIÓN EN SERVIU METROPOLITANO*

---

DEJA SIN EFECTO RESOLUCIÓN EXENTA Nº 3726 DE 2020, Y APRUEBA ACTUALIZACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR, EN EL CONTEXTO DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD, PARA SU APLICACIÓN EN SERVIU METROPOLITANO.

Departamento Programación Física y Control
Sistema de Seguridad de la Información
**OFPA N°** 188

**CON ESTA FECHA SE HA DICTADO LA SIGUIENTE:**

**RESOLUCIÓN EXENTA Nº** 371 05/02/2025

**SANTIAGO,**

**VISTOS:**

**a.** La Ley Nº 16.744 de 1968, del Ministerio del Trabajo y Previsión Social, que establece Normas Sobre Accidentes del Trabajo y Enfermedades Profesionales;

**b.** 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;

**c.** La Ley Nº 19.628 de 1999, sobre Protección de la Vida Privada, regula el tratamiento de los datos de carácter personal por organismos públicos o privados en registros o bancos de datos;

**d.** La Ley Nº 20.123/2006, del Ministerio del Trabajo y Previsión Social de Chile, regula el trabajo en régimen de subcontratación, el funcionamiento de las empresas de servicios transitorios y el contrato de trabajo de servicios transitorios;

**e.** La Ley Nº 20.285 de agosto 2008, del Ministerio Secretaría General de la Presidencia, Sobre Acceso a la Información Pública;

**f.** La Ley Nº 21.180 sobre Transformación Digital del Estado, promulgada con fecha 25 de octubre de 2019 y publicada con fecha el 11 de noviembre de 2019, que modifica las bases de los procedimientos administrativos para avanzar en su digitalización, contribuyendo así a la entrega de servicios más cercanos, simples y oportunos a la ciudadanía;

**g.** La Ley Nº 21.459 de fecha 20 de junio de 2022, del Ministerio de Justicia y Derechos Humanos, que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest;

**h.** La Ley Nº 21.634, de 2023 que moderniza la Ley N° 19.886 y otras leyes, para mejorar la calidad del gasto público, aumentar los estándares de probidad y transparencia e introducir principios de economía circular en las compras del estado, del Ministerio de Hacienda;

**i.** La Ley Nº 21.663 de fecha 8 de abril de 2024, del Ministerio del Interior y Seguridad Pública, que establece que establece la Ley de Marco de Ciberseguridad;

**j.** El Decreto Nº 236 del 2003. Aprueba Bases Generales Reglamentarias de Contratación de Obras para Los Servicios de Vivienda y Urbanización;

**k.** El Decreto Supremo Nº 83 de fecha 03 de junio 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;

**l.** El Decreto Supremo Nº 14 de fecha 15 de enero de 2014, del Ministerio de Economía, Fomento y Turismo, que modifica Decreto Nº 181/2002, que aprueba reglamento de la Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los Decretos que indica;

**m.** El Decreto Nº 83 de fecha 27 de abril de 2017, del Ministerio de Relaciones Exteriores, que promulga el Convenio sobre la Ciberdelincuencia;

**n.** El Decreto Nº 273 de fecha 13 de septiembre de 2022, del Ministerio del Interior y Seguridad Pública, que establece la obligación de Reportar Incidentes de Ciberseguridad;

**o.** El Decreto Nº 7 de fecha 17 de agosto de 2023, del Ministerio Secretaría General de la República, que Establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N° 21.180;

**p.** El Decreto Nº 164 de fecha 04 de diciembre de 2023, del Ministerio del Interior y Seguridad Pública, que Aprueba la Política Nacional de Ciberseguridad 2023-2028, que contiene los lineamientos políticos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2028, para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente;

**q.** 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;

**r.** El Instructivo Presidencial Nº 001 de fecha 24 de enero de 2019, que imparte instrucciones sobre Transformación Digital en los órganos de la Administración del Estado;

**s.** La Norma NCh-ISO 27001 de Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información – Requisitos;

**t.** La Resolución Exenta Nº 3726, de fecha 19 de noviembre de 2020, que actualiza y complementa Política de Seguridad de la Información para las Relaciones con el Proveedor, y su aplicación en SERVIU Metropolitano;

**u.** La Resolución Exenta Nº 4249 de fecha 11 de noviembre de 2024, que aprueba los Roles y Responsabilidades de la Estructura Funcional del Comité de Seguridad de la Información y Ciberseguridad en SERVIU Metropolitano;

**v.** La Resolución Exenta Nº 5225 de fecha 29 de diciembre de 2023, que aprueba integración de la versión Nº 09 de la Política General de la Información del Ministerio de Vivienda y Urbanismo y deja sin efecto anteriores versiones, en SERVIU Metropolitano;

**w.** La Resolución Nº 7 y 14, de fecha 26 de marzo de 2019 y 29 de diciembre de 2022, 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 singularizan quedarán sujetos a dicho trámite o a controles de remplazo cuando corresponda;

**x.** El Decreto Exento RA N° 272/84/2023 (V. y U.) de fecha 01 de diciembre de 2023, que me nombra Director del Servicio de Vivienda y Urbanización Metropolitano, y las facultades que en tal carácter me competen en conformidad al D.S N° 355 (V. y U.) del año 1976, Reglamento Orgánico de los SERVIU, dicto la siguiente:

**CONSIDERANDO:**

**a.** Que se han dictado una serie de normas en materia de Seguridad de la Información y Ciberseguridad en Chile, entre las que se encuentran aquellas singularizadas en los Vistos de las letras g), h), i), k), l), m), n), o), p), q), r) y s) de la presente Resolución Exenta a aprobación.

**b.** La necesidad de actualizar y complementar la Política de Seguridad de la Información para las Relaciones con el Proveedor, señalada en el visto t), es fundamental para el desarrollo de las actividades relacionadas con la Seguridad de la Información. Esto tiene como objetivo proteger la confidencialidad de los datos a los que las Entidades Proveedoras tienen acceso, garantizar la seguridad de la información, minimizar los riesgos y asegurar el cumplimiento normativo en SERVIU Metropolitano, alineándose con la Norma NCh-ISO 27001. Por lo tanto, dicto la siguiente:

**RESOLUCIÓN:**

I. **DÉJESE SIN EFECTO,** a partir de la total tramitación del presente acto administrativo, la Resolución Exenta N°3.726 de fecha 19 de noviembre de 2020, que actualiza y complementa la Política de Seguridad de la Información para las Relaciones con el Proveedor, y su aplicación en SERVIU Metropolitano;

II. **APRUÉBESE,** la actualización de la Política de Seguridad de la Información para las Relaciones con el Proveedor, perteneciente al Sistema de Seguridad de la Información, y aplíquese íntegramente a partir de la fecha en que sea formalizada la presente Resolución Exenta en SERVIU Metropolitano, el cual se define a continuación:

# 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 con la Seguridad de la Información para las Empresas Proveedoras 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 las Empresas Proveedoras 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.15.1.1 de la Norma NCh-ISO 27001, sobre Política de Seguridad de la Información para las Relaciones con el Proveedor.

## 3. ROLES Y RESPONSABILIDADES:

- A continuación, se detalla el esquema relacional de la Estructura funcional para la implementación y mantenimiento del Sistema de Seguridad de la Información y Ciberseguridad,[1] con la Identificación de sus miembros y sus responsabilidades, y que tienen un papel fundamental en la coordinación de decisiones, supervisión, desarrollo e implementación, en conformidad a la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo integrado en SERVIU Metropolitano.

### 3.1 DIRECTOR/A DEL SERVIU METROPOLITANO:

- Responsable de la supervisión general del Sistema de Seguridad de la Información y Ciberseguridad en SERVIU Metropolitano.


[1] Resol. Ex. de Roles y Responsabilidades de la Estructura Funcional del Comité de Seguridad de la Información y Ciberseguridad, aprobada y difundida en SERVIU Metropolitano.

### 3.2 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN:

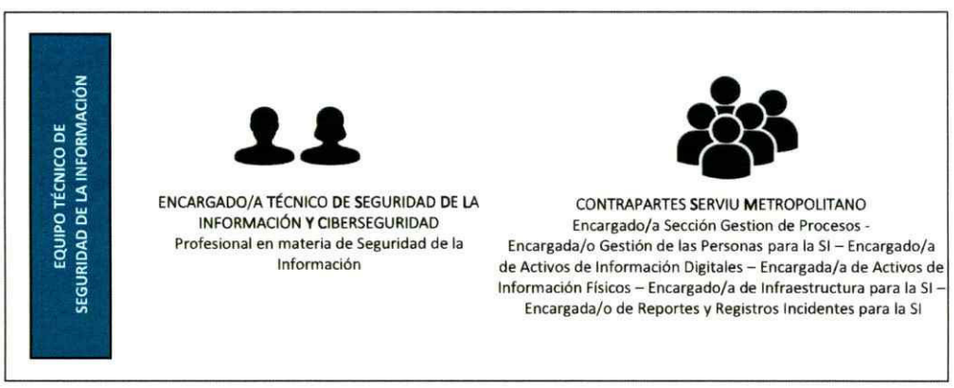
- Es el órgano de participación interna del Servicio responsable/encargado de asesorar en la implementación de procedimientos estándares que se desprenden de las Políticas en materia de Seguridad de la Información y Ciberseguridad en SERVIU Metropolitano.

- Está integrado por: el(la) Encargado/a de Seguridad de la Información y Ciberseguridad, el(la) Coordinador/a de Seguridad de la Información y Ciberseguridad, y las Jefaturas de la Subdirección de Vivienda y Equipamiento, Subdirección de Pavimentación y Obras Viales, Subdirección de Operaciones Habitacionales, Departamento Gestión Inmobiliaria, Subdirección Jurídica, Subdirección de Administración y Finanzas, Departamento Programación Física y Control, Contralora Interna y Sección Comunicaciones.


### 3.3 EQUIPO TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN:

- Conformado por el(la) Encargado/a Técnico de Seguridad de la Información y Ciberseguridad, y las Contrapartes en Seguridad de la Información y Ciberseguridad: Encargado/a Sección Gestion de Procesos, Encargada/o Gestión de las Personas para la Seguridad de la Información, Encargado/a de Activos de Información Digitales, Encargado/a de Activos de Información Físicos, Encargado/a de Infraestructura para la Seguridad de la Información, Encargada/o de Reportes y Registros Incidentes para la Seguridad de la Información.

- A continuación, se detalla la estructura funcional del Equipo Técnico de Seguridad de la Información, con sus roles y funciones, con el objeto de gestionar, establecer, implementar, mantener y mejorar continuamente la Documentación de Seguridad de la Información:



**4. DIRECTRICES:**

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

**4.1 Cumplimiento del Contrato:**

1. Se entenderá que todas las actividades desarrolladas por las Empresas Proveedoras que prestan servicios a SERVIU Metropolitano se encuentran establecidas en los respectivos Contratos de Provisión de Servicios que se vinculan a este.

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

3. De acuerdo con lo establecido en las cláusulas asociadas al Contrato de Provisión de Servicios, toda Empresa Proveedora que desarrolle labores para SERVIU Metropolitano deberá cumplir con lo definido en las Políticas y Procedimientos del Sistema de Seguridad de la Información y Ciberseguridad de SERVIU Metropolitano.

4. 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 Acceso a Equipos de Tecnologías de Información (TI):**

1. Las instalaciones de sistemas, equipos de comunicación y/o programas en los computadores deben ser autorizados por la Sección Informática del Servicio. Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de información propia del Servicio sin la debida autorización.

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

3. La Empresa Proveedora se compromete a utilizar los recursos dispuestos dentro de la Institución para la provisión del servicio, de acuerdo con las condiciones establecidas en cada uno de los procesos.

4. Los recursos proporcionados por SERVIU Metropolitano al personal externo, sin importar su naturaleza (informáticos, datos, software, redes, sistemas de comunicación, materiales, herramientas, implementos de seguridad y sanitarios, etc.), están disponibles exclusivamente para apoyar las obligaciones y el propósito operativo para los cuales fueron destinados.

- El(la) Encargado/a de la Sección Informática y la Jefatura del Departamento de Servicios Generales implementarán mecanismos de control, con la finalidad de verificar el uso adecuado de estos.

5. Los equipos computacionales propios de las Empresas Proveedoras 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 con el contrato.

6. 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 Técnica 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.

7. La Empresa Proveedora 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. La Empresa Proveedora nunca podrá crear carpetas temporales en unidades locales del equipo computacional asignado por el Servicio.

8. La Empresa Proveedora 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:**

1. Las Empresas Proveedoras 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 (https://serviumetropolitana.minvu.gob.cl/).

2. La Empresa Proveedora 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.

3. La Empresa Proveedora 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.

4. 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.

5. La Empresa Proveedora 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.

- La Empresa Proveedora 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 con las normas legales vigentes.

6. La divulgación, por cualquier medio, de la información antes referida por parte de la Empresa Proveedora, 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.

- 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 Metropolitano.

- 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 facultará al SERVIU Metropolitano para dar por terminado el contrato de manera anticipada y emprender las acciones judiciales pertinentes.

**5. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN:**

- La evaluación y revisión de la Política General de Seguridad de la Información y sus políticas específicas, procedimientos y normativas que integran el Sistema de Seguridad de la Información y Ciberseguridad, deberá efectuarse, al menos una vez al año por el Comité de Seguridad de la Información y Ciberseguridad, 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. De no existir cambios significativos en el Servicio las reuniones semestrales del Comité de seguridad de la Información y Ciberseguridad serán consideradas proceso de revisión por la Dirección.

- La formalización, modificación y actualización del presente documento, así como toda la documentación vinculada al Sistema de Seguridad de la Información y Ciberseguridad, 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 y Ciberseguridad, será comunicada a través de los canales de difusión establecidos, pudiendo ser por correo electrónico, publicación en la INTRANET, u otro medio que la Institución considere pertinente, asegurando que el contenido de la documentación sea accesible y comprensible para todo el personal del SERVIU Metropolitano.

- Cada vez que SERVIU Metropolitano realice un proceso de contratación de servicio con alguna Empresa Proveedora, 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.

- En el caso que se licite la ejecución de una Obra al interior de las dependencias del Servicio, la Sección Propuestas del Departamento de Programación Física y Control, 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.

- Adicionalmente, la Política General como las Políticas Específicas de Seguridad de la Información y Ciberseguridad se encuentran publicadas en la página web institucional, disponible para consulta permanente del funcionariado o personal externo que prestan servicios para el SERVIU Metropolitano, por lo que se entenderá conocido por todos.

**7. SANCIONES APLICABLES:**

- El presente documento tiene su base en las definiciones, términos y controles descritos en la Norma Chilena NCh-ISO 27001 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 la presente Política y toda documentación vinculada al Sistema de Seguridad de la Información y Ciberseguridad, debidamente acreditado, conllevará a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los(as) 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 y Ciberseguridad, 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 con 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 el(la) Encargado/a de la Seguridad de la Información y Ciberseguridad y enviará al Comité de Seguridad de la Información y Ciberseguridad del Servicio, para la toma de conocimiento.

**9. DOCUMENTOS RELACIONADOS:**

- La Ley Nº 16.744 de 1968, del Ministerio del Trabajo y Previsión Social, que establece Normas Sobre Accidentes del Trabajo y Enfermedades Profesionales.
- La Ley Nº 19.628 de 1999, sobre Protección de la Vida Privada, regula el tratamiento de los datos de carácter personal por organismos públicos o privados en registros o bancos de datos.
- La Ley Nº 19.886 de 2003 de Bases sobre Contratos Administrativos de Suministros y Prestación de Servicios, del Ministerio de Hacienda.

- La Ley Nº 20.123/2006, del Ministerio del Trabajo y Previsión Social de Chile, 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 20.285 de agosto 2008, del Ministerio Secretaría General de la Presidencia, Sobre Acceso a la Información Pública.
- El Decreto Nº 236 del 2003. Aprueba Bases Generales Reglamentarias de Contratación de Obras para Los Servicios de Vivienda y Urbanización.
- Ley N° 21.180 sobre Transformación Digital del Estado, publicada el 11 de noviembre de 2019, modifica las bases de los procedimientos administrativos para avanzar en su digitalización, contribuyendo así a la entrega de servicios más cercanos, simples y oportunos a la ciudadanía.
- Ley Nº 21.459 de fecha 20 de junio de 2022, del Ministerio de Justicia y Derechos Humanos, que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
- Ley Nº 21.663 de fecha 8 de abril de 2024, del Ministerio del Interior y Seguridad Pública, que establece que establece la Ley de Marco de Ciberseguridad e Infraestructura Crítica de la Información en Chile.
- Decreto Supremo Nº 83 de fecha 03 de junio 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.
- Decreto Supremo Nº 14 de fecha 15 de enero de 2014, del Ministerio de Economía, Fomento y Turismo, que modifica Decreto Nº 181/2002, que aprueba reglamento de la Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los Decretos que indica.
- Decreto Nº 83 de fecha 27 de abril de 2017, del Ministerio de Relaciones Exteriores, que promulga el Convenio sobre la Ciberdelincuencia.
- Decreto Nº 273 de fecha 13 de septiembre de 2022, del Ministerio del Interior y Seguridad Pública, que establece la obligación de Reportar Incidentes de Ciberseguridad.
- Decreto Nº 7 del año 2023, del Ministerio Secretaría General de la República, que Establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N° 21.180.
- Decreto Nº 164 del 04 de diciembre del 2023, del Ministerio del Interior y Seguridad Pública, que Aprueba la Política Nacional de Ciberseguridad 2023-2028, que contiene los lineamientos políticos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2028, para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente.
- 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.
- Instructivo Presidencial Nº 001 de fecha 24 de enero de 2019, que imparte instrucciones sobre Transformación Digital en los órganos de la Administración del Estado.
- Norma NCh-ISO 27001 de Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.
- Resolución Exenta que aprueba integración de la Política General de Seguridad de la Información del Ministerio de Vivienda y Urbanismo, para su aplicación en SERVIU Metropolitano.
- Resolución de Roles y Responsabilidades de la Estructura Funcional del Comité de Seguridad de la Información y Ciberseguridad, para su aplicación en SERVIU Metropolitano.
- Política de Dispositivos Móviles, y su aplicación en SERVIU Metropolitano.
- Política de Control del Acceso Físico, y su aplicación en SERVIU Metropolitano.
- Política de Control del Acceso Lógico, y su aplicación en SERVIU Metropolitano.
- Procedimiento Perímetros de Seguridad Física P-SSI-06, de SERVIU Metropolitano.
- Procedimiento Gestión de Incidentes de Seguridad de la Información del Ministerio de Vivienda y Urbanismo, para su aplicación en SERVIU Metropolitano.

**10. CONTROL DE VERSIONES:**

| N° Versión | Fecha | Principales puntos modificados |
|---|---|---|
| 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 | Resolución Exenta N° 3726 de fecha 19.11.2020. Actualiza y complementa Política de Seguridad de la Información para las Relaciones con el Proveedor, y su aplicación en SERVIU Metropolitano. |

III. **ESTABLÉCESE,** 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 alguna Empresa Proveedora.

IV. **ESTABLÉCESE,** que la presente Resolución Exenta actualiza la Política de Seguridad de la Información para las Relaciones con el Proveedor, para el Sistema de Seguridad de la Información y Ciberseguridad, y, será almacenada en el sitio del Sistema de Seguridad de la Información ubicado en la INTRANET del Servicio y, difundido al funcionariado a través de mecanismos de la comunicación interna existentes en SERVIU Metropolitano.

V. **EJECÚTESE,** por el(la) Encargado/a de la Sección Adquisiciones de la Subdirección de Administración y Finanzas en coordinación con el Comité de Seguridad de la Información y Ciberseguridad del SERVIU Metropolitano, de velar y garantizar el cumplimiento estricto de este documento, que ha sido ratificada por la presente Resolución Exenta.

VI. **DÉJESE** constancia, que la presente Resolución no afecta el presupuesto del Servicio.

**ANÓTESE, NOTIFÍQUESE Y CÚMPLASE**

SERVICIO DE VIVIENDA Y URBANIZACIÓN REGIÓN METROPOLITANA DIRECTOR

**ROBERTO ACOSTA KERUM**
**DIRECTOR**
**SERVIU METROPOLITANO**

Alejandra Hermosilla Hurtado — Claudia Ramírez Saldias — Daniela Montenegro Bravo — Roberto Márquez Alvarado

**AHH/ CRS/ CCR / DMB / EMA/**

**TRANSCRIPCIÓN:**

1. Subdirección de Administración y Finanzas.
2. Subdirección de Pavimentación y Obras Viales.
3. Subdirección de Vivienda y Equipamiento.
4. Subdirección de Operaciones Habitacionales.
5. Subdirección Jurídica.
6. Departamento Programación Física y Control.
7. Departamento Gestión Inmobiliaria.
8. Contraloría Interna SERVIU Metropolitano.
9. Ministro de Fe.
10. Sección Partes y Archivo.
11. Sección Gestión de Procesos.

NO AFECTA PRESUPUESTO
M. Trinidad Díaz V.
30 DICIEMBRE 2024
Subdepartamento de Presupuesto
Subdirección de Adm. Y Finanzas

MINISTRO DE FE

**FANCY HUERTA LABARCA**
**Ministro de Fe - Subrogante**