DEJA SIN EFECTO LA RESOLUCIÓN EXENTA N°1508, (V. Y U.), DE 08-09-2023 Y LA RESOLUCIÓN EXENTA N° 325, (V. Y U.), DE 04-03-2025, Y APRUEBA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD, PARA LA SUBSECRETARÍA DE VIVIENDA Y URBANISMO, SUS SECRETARIAS REGIONALES MINISTERIALES, LOS SERVICIOS DE VIVIENDA Y URBANIZACIÓN Y EL PARQUE METROPOLITANO DE SANTIAGO. -

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARÍA
13 ENE 2026
RESOLUCIÓN EXENTA
TRAMITADA

SANTIAGO, 13 ENE. 2026
HOY SE RESOLVIO LO QUE SIGUE

RESOLUCIÓN EXENTA N° 044

VISTOS: Lo dispuesto en la Ley N°16.391, que crea el Ministerio de Vivienda y Urbanismo; en el D.L. N°1.305 de 1975 que Reestructura y Regionaliza el Ministerio de Vivienda y Urbanismo; la Ley N°19.628 sobre Protección de la Vida Privada y su texto modificatorio la Ley N° 21.719 que regula la Protección y el Tratamiento de Datos Personales y crea la Agencia de Protección de Datos Personales; la ley N°19.880 que establece Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado; la Ley N° 20.285 sobre Acceso a la Información Pública; la Ley N°21.180 sobre Transformación Digital del Estado; la Ley N° 21.658 que Crea la Secretaría de Gobierno Digital en la Subsecretaría de Hacienda, y adecúa los Cuerpos legales que indica; la Ley N°21.663, sobre Ley Marco de Ciberseguridad; el D.S. N°83, de 2005, del Ministerio Secretaria 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; el 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°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 Secretaria General de la Presidencia, que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N°21.180; el D.S. N°164 de 2023, del Ministerio del Interior y Seguridad Pública, que aprobó la Política Nacional de Ciberseguridad 2023-2028; la Norma Chilena NCh-ISO 27001:2023 que define los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, dentro del contexto de una organización; la Resolución Exenta N° 325, (V. y U.), de 2025, que modifica la Resolución Exenta N° 1508 (V. y U.), de 2023 y Aprueba la Política General de Seguridad de la Información para la Subsecretaría de Vivienda y Urbanismo, sus Secretarias Regionales Ministeriales, los Servicios de Vivienda y Urbanización y el Parque Metropolitano de Santiago; 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; y, la Resolución N°36 de 2024, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón;

MINISTERIO DE VIVIENDA Y URBANISMO
DIVISIÓN JURÍDICA

MINISTERIO DE VIVIENDA Y URBANISMO
VERONICA IBACACHE
Jefa
DIVISIÓN JURÍDICA

CONSIDERANDO:

a) Que, con el advenimiento de transformación digital del Estado al tenor de los dispuesto en la Ley N°21.180 y demás normativa señalada pormenorizadamente en los Vistos de esta resolución, es necesario aprobar administrativamente materias relevantes referidas a Ciberseguridad, Seguridad de la Información, Gobernanza de Datos, y protección de la Vida Privada y de Datos Personales, para lo cual se requiere elaborar actos administrativos de contenido claro, a través de una técnica jurídica que permita comprender cabalmente su contenido y, en su caso, las eventuales modificaciones que en ellos se realice con posterioridad;

b) Que la Resolución Exenta N°325, (V. y U.), de 04 de marzo de 2025, citada en la parte final de los Vistos de esta resolución, está redactada de una manera poco clara al aprobar la Política General de Seguridad de la Información Versión 10;

c) Que, es preciso dictar una nueva resolución que apruebe la Política General de Seguridad de la Información para la Subsecretaría de Vivienda y Urbanismo, sus SEREMI, SERVIU y Parque Metropolitano de Santiago, que dé cuenta de un texto claro susceptible de ser debidamente actualizado a futuro;

d) La necesidad evaluada como resultado de la revisión efectuada por el Comité de Seguridad de la Información, de reestructurar y ajustar contenidos en la Política de Seguridad de la Información de la Versión 10, aprobada mediante la Resolución Exenta N° 1508, (V. y U.), de 2023.

RESUELVO:

1. DÉJASE sin efecto la Resolución Exenta N°1508, (V. y U.), de 08 de septiembre de 2023, y la Resolución Exenta N° 325, (V. y U.), de 04 de marzo de 2025, a partir de la total tramitación del presente acto administrativo.

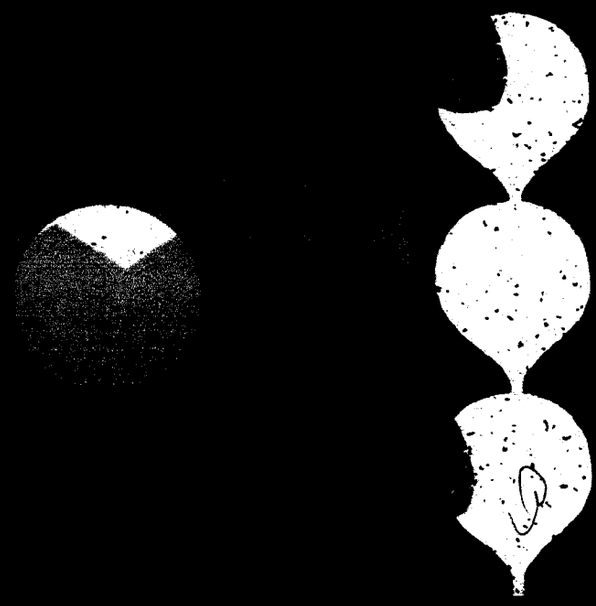
2. APRUÉBASE la Política General de Seguridad de la Información y Ciberseguridad del Ministerio de Vivienda y Urbanismo, **Versión 11**, para ser implementada en la Subsecretaría de Vivienda y Urbanismo, en las 16 Secretarías Regionales Ministeriales de Vivienda y Urbanismo, en los 16 Servicios de Vivienda y Urbanización y en el Parque Metropolitano de Santiago, que se detalla a continuación:

MINISTERIO DE VIVIENDA Y URBANISMO
Ma. MALEKA GARCIA M.
Abogado
DIVISIÓN JURÍDICA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Versión 11

Ministerio de Vivienda y Urbanismo
Diciembre, 2025



Ministerio de Vivienda y Urbanismo

Gobierno de Chile

MINISTERIO DE VIVIENDA Y URBANISMO
Ma. VALESKA GATICA N.
Abogado
DIVISIÓN JURÍDICA

CONTENIDO

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.
Activo Crítico / Activo Esencial (recomendado por Ley 21.663)	Activo cuya indisponibilidad, alteración o pérdida puede afectar significativamente la continuidad operativa institucional, la prestación de servicios esenciales o la seguridad de la información.
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.
Datos personales	Información concerniente a personas naturales, identificadas o identificables, conforme a la Ley N° 19.628.
Datos sensibles	Datos personales que se refieren a características físicas o morales de las personas, o a hechos o circunstancias de su vida privada o intimidad, cuyo tratamiento requiere resguardos reforzados.
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 la Seguridad de la Información, Ciberseguridad y Gobernanza de Datos en adelante, SSI, de la organización y aplicables al mismo, así como el rol de cada institución del Ministerio de Vivienda y Urbanismo.
Dueño del Dato (Data Owner)	Responsable de un conjunto específico de datos dentro de la organización, definiendo su calidad, seguridad, uso y valor para asegurarse que se alinee con los objetivos estratégicos y se trate como un activo valioso.

Custodio del dato	Persona o unidad responsable de administrar sistemas, plataformas o bases de datos, implementando las directrices de seguridad definidas por el Dueño del Dato.
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	Evento o serie de eventos inesperados que comprometen o pueden comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de sistemas, datos o servicios institucionales.
Incidente Significativo de Ciberseguridad (Ley 21.663)	Aquel que, por su severidad, impacto o alcance, afecta o puede afectar la prestación de servicios esenciales, la continuidad operativa o la infraestructura crítica, y que debe ser notificado a la ANCI y al CSIRT de Gobierno.
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")	Conjunto de software, datos, interfaces, servicios y componentes tecnológicos que soportan un proceso institucional.
Resiliencia Digital	Capacidad de los sistemas, plataformas y servicios tecnológicos para resistir, recuperarse y continuar operando frente a fallas, incidentes, ciberataques o interrupciones.
Riesgo	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.
Trazabilidad	Capacidad de registrar, seguir, monitorear y reconstruir acciones realizadas sobre sistemas, activos y datos, permitiendo auditoría, investigación y rendición de cuentas.

Usuarios(as)	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, que acceden a sistemas, servicios digitales o información institucional.

1. DECLARACIÓN INSTITUCIONAL

El Ministerio de Vivienda y Urbanismo (MINVU) declara su compromiso permanente con la protección de los activos de información, los servicios tecnológicos, los datos institucionales y la continuidad operativa, mediante la implementación y mejora continua de un Sistema de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos, en adelante SSI.

Este compromiso busca resguardar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y resiliencia digital de los servicios institucionales, de acuerdo con las obligaciones establecidas por la legislación vigente y los estándares técnicos aplicables[1].

El MINVU reconoce que la seguridad de la información es fundamental para cumplir los objetivos institucionales y para entregar servicios confiables, seguros y oportunos a la ciudadanía.

Por tal motivo la información es un activo esencial para que el MINVU avance hacia el cumplimiento de su misión ministerial.

2. OBJETIVO GENERAL

La presente Política tiene por finalidad establecer el marco rector que orienta la seguridad de la información, la ciberseguridad y la gobernanza de datos en el Ministerio de Vivienda y Urbanismo (MINVU) y sus organismos relacionados, definiendo los principios estratégicos, responsabilidades y lineamientos necesarios para el funcionamiento del Sistema de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos (SSI).

Asimismo, esta Política establece un marco que se complementa con la Política General de Seguridad Tecnológica y Servicios Digitales (PGST), las políticas específicas y los procedimientos operativos que conforman el SSI, asegurando la adecuada gestión de riesgos y el cumplimiento de la normativa aplicable.

2.1 Objetivos específicos de la seguridad de la información, Ciberseguridad y Gobernanza de datos.

El Sistema de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos se alinean y dan soporte a los objetivos estratégicos ministeriales definidos en la Ficha de Definiciones Estratégicas A0. En este marco, la institución establece los siguientes objetivos específicos:

- Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la Seguridad de la Información y Ciberseguridad.
- Proteger los activos de información, sistemas, servicios digitales y procesos institucionales frente a amenazas internas y externas, fortaleciendo su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Asegurar que los datos institucionales sean gestionados conforme a principios de calidad, seguridad, trazabilidad y uso legítimo, en coherencia con el Modelo Institucional de Gobernanza de Datos.
- Mantener un enfoque basado en riesgos, permitiendo priorizar controles y medidas de seguridad de acuerdo con la criticidad de los activos, procesos y servicios institucionales.

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

- Garantizar la continuidad operativa y la resiliencia digital, mediante mecanismos de prevención, respuesta y recuperación ante incidentes que puedan afectar la provisión de servicios esenciales.
- Promover una cultura institucional de seguridad y conducta digital responsable, fortaleciendo capacidades, buenas prácticas y el cumplimiento normativo en todo el personal.
- Dar cumplimiento a las obligaciones establecidas en la Ley N° 21.663, especialmente en materia de implementación de medidas mínimas de ciberseguridad, gestión y notificación de incidentes significativos, y cooperación con el CSIRT de Gobierno y la ANCI.
- Establecer niveles de acceso adecuados a la información, brindando y asegurando la preservación de la confidencialidad, integridad y disponibilidad que requiera cada sistema, proceso, actividad crítica y usuario.
- Desarrollar y mantener un marco de Gestión de Riesgo Cibernético, aplicable a sistemas, procesos y actividades críticas, que permita resguardar el cumplimiento de los objetivos estratégicos ministeriales.
- Formalizar y mantener controles, políticas, procesos y procedimientos, seleccionados mediante procesos de gestión de riesgos, destinados a proteger los activos de información y asegurar la implementación efectiva del SSI.

Para el cumplimiento de estos objetivos, en el marco del SSI se establecerá un conjunto de controles aplicables, formalizados mediante políticas, procesos y procedimientos, en consistencia con los principios establecidos en esta Política.

3. MARCO NORMATIVO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y GOBERNANZA DE DATOS

El Sistema de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos del MINVU (SSI) se sustenta en los siguientes marcos normativos y estándares:

- Ley N° 21.663 sobre Ciberseguridad.
- Ley N° 19.628 sobre Protección de Datos Personales.
- Ley N° 21.180 sobre Transformación Digital.
- Decreto Supremo N° 7/2023.
- NCh-ISO/IEC 27001:2022.
- NCh-ISO/IEC 27002:2022.
- NIST Cybersecurity Framework 2.0.
- Directrices de ANCI y CSIRT de Gobierno.

Complementariamente, se considera lo establecido en el Catastro de Normativa SSI elaborado por la División Jurídica de la Subsecretaría de V. y U.

4. AMBITO DE APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD – ALCANCE

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

4.1. Alcance Institucional

La presente Política es de cumplimiento obligatorio para:

- La Subsecretaría de Vivienda y Urbanismo.
- Las Secretarías Regionales Ministeriales de Vivienda y Urbanismo (SEREMI).
- Los Servicios de Vivienda y Urbanización (SERVIU) Regionales.
- El Parque Metropolitano de Santiago.
- Todo el personal del MINVU y sus Servicios: funcionarios/as de planta, contrata y honorarios.
- Asesores, consultores, proveedores, personal externo, pasantes y cualquier persona natural o jurídica que mantenga relación contractual o que preste servicios al MINVU.
- Independiente de la modalidad de trabajo utilizada (presencial, a distancia, teletrabajo u otras).

Asimismo, la Política aplica a:

- Todos los sistemas, plataformas, aplicaciones, servicios digitales e infraestructura tecnológica, ya se encuentren alojados en dependencias institucionales o en entornos de computación en la nube, propios o administrados por terceros.
- Todos los datos, documentos e información institucional, cualquiera sea su formato, soporte o medio de almacenamiento.
- Procesos, actividades, procedimientos y productos estratégicos asociados al cumplimiento de los objetivos ministeriales.
- Sistemas y servicios provistos por terceros que procesen, almacenen o transmitan información institucional, especialmente cuando sean considerados críticos o esenciales para la operación del Ministerio.

4.2. Relación con el Sistema de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos (SSI)

El Sistema de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos (SSI) del MINVU se organiza mediante la siguiente estructura documental:

1. Política General de Seguridad de la Información (este documento)
2. Política General de Seguridad Tecnológica y Servicios Digitales (PGST)
3. Política Específica de Gobernanza de Datos
4. Políticas específicas de seguridad (P.01 a P.14 u otras que se incorporen)
5. Procedimientos técnicos y operativos
6. Guías, instructivos y estándares institucionales

La PGST regula los controles tecnológicos y operativos, mientras que esta Política establece los principios, responsabilidades y el marco de gobernanza que orienta al conjunto del SSI, asegurando coherencia normativa y una gestión integral de riesgos de seguridad y ciberseguridad.

5. GOBERNANZA Y ROLES DEL SSI

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 un **Encargado/a de Seguridad de la Información**, un **Comité de Seguridad de la Información** o Comité de similar denominación y un ***Encargado/a de Activos de Información,***

A continuación, se describen las responsabilidades que debe tener cada rol para el funcionamiento del SSI:

ROL / UNIDAD	RESPONSABILIDADES PRINCIPALES
Subsecretaría de Vivienda y Urbanismo	Aprueba esta Política. Supervisa su cumplimiento institucional.
Comité de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos	Órgano asesor y decisor en materias estratégicas de seguridad. Aprueba lineamientos. Revisa riesgos e incidentes relevantes.
Encargado/a de Seguridad de la Información (CISO) Para el caso de Subsecretaría de V. y U. corresponde a Encargado/a de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos	Liderar la implementación del SSI. Coordinar con ANCI y CSIRT. Supervisar cumplimiento normativo. Presentar reportes estratégicos al Comité.

ROL / UNIDAD	RESPONSABILIDADES PRINCIPALES
División Informática (DINFO)	Implementar controles tecnológicos definidos por la PGST. Administrar infraestructura, accesos, redes, respaldos y plataformas. Mantener evidencias y registros técnicos de seguridad.
Dueños de Datos	Clasificar la información. Autorizar accesos. Definir requerimientos de seguridad. Validar restauraciones y uso de datos.
Custodios de Datos	Administrar sistemas y plataformas bajo directrices del Dueño del Dato. Implementar los controles correspondientes.
Coordinadores/as Informáticos Regionales	Aplicar controles y lineamientos del SSI en su jurisdicción.
Encargado/a de Activos de Información	Responsable de la identificación y clasificación de los activos de información, 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.
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 y proteger credenciales y accesos.

6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

El Ministerio de Vivienda y Urbanismo (MINVU) adopta los siguientes principios estratégicos para la gestión de la seguridad de la información y la ciberseguridad, los cuales guían el funcionamiento del Sistema de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos (SSI) y orientan la definición de políticas específicas, procedimientos y controles técnicos:

6.1. Confidencialidad

La información institucional debe ser accedida únicamente por personas, sistemas o procesos autorizados, mediante mecanismos de control que prevengan su uso, modificación o divulgación no autorizada, en cumplimiento de la normativa vigente, incluyendo la Ley N° 19.628 y la Ley N° 20.285.

6.2. Integridad

La información debe mantenerse exacta, completa, coherente y protegida frente a alteraciones no autorizadas. Los sistemas y procesos institucionales deberán asegurar la trazabilidad de cambios y la verificación periódica de la consistencia de los datos.

6.3. Disponibilidad

La información, servicios digitales y activos tecnológicos deben estar accesibles y operativos cuando sean requeridos para el cumplimiento de las funciones institucionales, considerando medidas de continuidad operativa, recuperación ante incidentes y resiliencia digital.

6.4. Autenticidad y No Repudio

El MINVU deberá asegurar que la identidad de usuarios, dispositivos, servicios o procesos sea verificada mediante mecanismos de autenticación confiables, y que las acciones críticas queden registradas de forma tal que no puedan ser negadas posteriormente.

6.5. Trazabilidad

Todas las acciones relevantes ejecutadas sobre sistemas, datos o servicios digitales deben ser registradas, monitoreadas y revisadas conforme a criterios de auditoría y control, permitiendo detectar, investigar y responder ante incidentes o actividades sospechosas.

6.6. Enfoque Basado en Riesgos

Las decisiones de seguridad deberán fundamentarse en procesos sistemáticos de identificación, análisis, evaluación y tratamiento de riesgos, priorizando medidas que protejan los activos más críticos y mitiguen los riesgos más significativos para la institución.

6.7. Seguridad por Diseño y por Defecto

Las soluciones tecnológicas, sistemas, servicios digitales y procesos institucionales deberán

incorporar medidas de seguridad desde su concepción y configuración inicial, garantizando que la protección de datos, la minimización de riesgos y los controles técnicos sean aplicados de forma preventiva.

6.8. Privacidad por Diseño y por Defecto

Toda actividad que implique tratamiento de datos personales deberá integrar controles que aseguren su protección desde las etapas iniciales del diseño de procesos, sistemas y servicios, promoviendo el uso proporcional y legítimo de dichos datos conforme a la Ley N° 19.628 y la normativa aplicable.

6.9. Zero Trust

El MINVU adopta el principio de "nunca confiar, siempre verificar", por lo que ningún usuario, dispositivo, red o servicio será considerado confiable por defecto. Todo acceso deberá ser verificado, autenticado, autorizado y monitoreado continuamente.

6.10. Resiliencia Digital

Los servicios, plataformas y activos críticos deben ser diseñados y operados para resistir, recuperarse y continuar funcionando frente a fallas, ciberataques, desastres o interrupciones, integrando capacidades de redundancia, respaldo y recuperación rápida.

6.11. Responsabilidad Compartida

En entornos de servicios en la nube, externalización o provisión tecnológica por terceros, la seguridad se entenderá bajo un modelo de responsabilidades compartidas, en el que cada parte deberá cumplir los controles que le sean propios, según contratos, normativa y marcos de referencia aplicables.

6.12. Ciclo de Vida Seguro de Activos y Datos

Los activos tecnológicos y los datos institucionales deberán ser gestionados responsablemente desde su creación hasta su eliminación, asegurando su protección, almacenamiento seguro, retención adecuada, destrucción segura y cumplimiento regulatorio durante todo su ciclo de vida.

6.13. Consideraciones para sistemas legados y heredados

Cuando sistemas o plataformas heredadas no puedan cumplir plenamente con los principios establecidos en esta Política, la División de informática de la Subsecretaría, en coordinación con los Dueños y Custodios de Datos, deberá identificar las brechas e incorporarlas en el proceso institucional de gestión de riesgos.

Cuando sea técnicamente posible, se aplicarán controles compensatorios para mitigar los riesgos, tales como restricciones de acceso, monitoreo reforzado, segmentación de red y auditorías periódicas.

Estos sistemas deberán incluirse en un plan de adecuación gradual que priorice su actualización, migración o reemplazo. La existencia de limitaciones técnicas no exime a las unidades responsables de aplicar medidas de resguardo razonables ni de reportar incidentes o vulnerabilidades asociadas a dichos sistemas.

7. GESTIÓN DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y GOBERNANZA DE DATOS

7.1. Elaboración de políticas y documentos del Sistema

La Política General de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos, así como las políticas específicas, procedimientos, instructivos y demás documentos del Sistema, deberán elaborarse conforme a los formatos institucionales estandarizados definidos para tal efecto, los cuales se mantendrán disponibles en los espacios oficiales habilitados, como el sitio del Sistema de Seguridad de la Información, el Banco de Procesos u otros que se determinen.

Para operacionalizar las políticas específicas, los Servicios podrán elaborar procedimientos, instructivos y otros instrumentos complementarios. Estos deberán ajustarse a los lineamientos de documentación institucional, mantener coherencia con esta Política y cumplir el marco normativo vigente.

7.2. Aprobación de políticas y documentos

La Política General de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos y las Políticas Específicas de Seguridad deberán ser aprobadas mediante acto administrativo suscrito por el Jefe de Servicio, facultad que no puede ser delegada.

Los demás documentos del Sistema —tales como normativas internas, procedimientos, instructivos y otros instrumentos operativos— serán aprobados mediante acto administrativo suscrito por el Jefe de Servicio o por la autoridad que cuente con delegación formal, conforme a la estructura organizacional, los niveles de responsabilidad y los lineamientos de seguridad definidos en cada Servicio.

7.3. Difusión y acceso a la documentación.

Esta Política y la documentación asociada al Sistema deberán ser difundidas y puestas a disposición del personal, garantizando que su contenido sea accesible, comprensible y pertinente para el adecuado ejercicio de las funciones institucionales.

La difusión se realizará a través de los canales institucionales establecidos, pudiendo considerar, entre otros, su publicación en el sitio del Sistema de Seguridad de la Información, Minvuletín, correos institucionales, afiches, material informativo u otros medios que cada Servicio estime pertinentes.

Adicionalmente, la Política General y aquellas Políticas Específicas de aplicación transversal estarán disponibles en el sitio web institucional, para consulta del personal, de terceros que prestan servicios al Ministerio y de la ciudadanía, según corresponda.

7.4. Revisión y evaluación de la Política.

La Política General de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos deberá ser revisada al menos una vez al año, o cuando lo solicite el Encargado/a de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos del MINVU o de uno o más Servicios, con el fin de asegurar su vigencia, adecuación e idoneidad.

En dicha revisión se considerarán, entre otros factores:

- Cambios en lineamientos estratégicos u organizacionales.
- Modificaciones relevantes en procesos, sistemas o actividades críticas.
- Cambios significativos en infraestructura o en el soporte tecnológico.
- Variaciones en los niveles de riesgo que afecten los activos de información.
- Cambios en leyes, reglamentos y normativa aplicable.
- Recomendaciones de autoridades competentes, auditorías u organismos externos.
- Evolución de amenazas, vulnerabilidades y tendencias en materia de ciberseguridad.

Asimismo, cada Servicio deberá evaluar el cumplimiento de la presente Política, a lo menos cada tres años, mediante auditorías internas, auditorías externas y/o revisiones independientes, conforme a sus planes de aseguramiento y control.

8. COMPROMISOS EN CIBERSEGURIDAD (Ley 21.663).

En el marco de las obligaciones establecidas por la Ley N° 21.663 sobre Ciberseguridad, y sin perjuicio de la normativa sectorial aplicable, el MINVU asume los siguientes compromisos institucionales:

8.1. Notificar oportunamente los incidentes de ciberseguridad significativos a la Agencia Nacional de Ciberseguridad (ANCI) y al CSIRT de Gobierno, dentro de los plazos y conforme a los procedimientos que dichas autoridades establezcan.

8.2. Mantener un inventario actualizado y completo de activos tecnológicos, servicios digitales e infraestructuras críticas, identificando aquellos cuya indisponibilidad o alteración pueda afectar la continuidad operativa institucional o la prestación de servicios esenciales.

8.3. Implementar y mantener las medidas mínimas de ciberseguridad definidas por la ANCI, así como los lineamientos técnicos, estándares o controles adicionales que resulten necesarios para reforzar la protección de los servicios y activos críticos.

8.4. Realizar los procesos de categorización de infraestructuras esenciales, cuando corresponda, de acuerdo con los criterios establecidos por la Ley N° 21.663 y las directrices emitidas por la autoridad competente.

8.5. Colaborar activamente con la ANCI, el CSIRT de Gobierno y otros organismos reguladores, facilitando la información, antecedentes y apoyo técnico que se requiera para la prevención, gestión y respuesta frente a incidentes de ciberseguridad.

8.6. Integrar la ciberseguridad como componente transversal de la gestión institucional, incorporándola en los procesos de planificación, gestión de riesgos, continuidad operativa, evaluación de proveedores y desarrollo de servicios digitales.

8.7. Promover una cultura organizacional de ciberseguridad, fortaleciendo capacidades técnicas, prácticas seguras de uso de sistemas y la conciencia del personal respecto de amenazas y obligaciones regulatorias.

9. CUMPLIMIENTO, FISCALIZACIÓN Y SANCIONES.

El incumplimiento de las obligaciones establecidas en esta Política de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos, así como de las políticas específicas y procedimientos asociados, por parte de los funcionarios del MINVU, SEREMI, SERVIU y PARQUEMET, constituye una

falta susceptible de generar responsabilidad administrativa. En tales casos, podrán aplicarse las medidas disciplinarias previstas en el Estatuto Administrativo, tales como censura, multa, suspensión o destitución, previo desarrollo del correspondiente Procedimiento Administrativo Disciplinario, según corresponda.

Cuando las infracciones sean cometidas por personas naturales o jurídicas que presten servicios al MINVU y que no estén sujetas a responsabilidad administrativa, podrá aplicarse el término anticipado del contrato u otras sanciones estipuladas en las condiciones contractuales, por incumplimiento de las obligaciones relacionadas con la seguridad de la información o la ciberseguridad.

Las sanciones anteriores se aplicarán sin perjuicio de las responsabilidades civiles, penales o de otra naturaleza que pudieran derivarse de acciones u omisiones que afecten la seguridad de la información institucional, especialmente en los casos en que dichas conductas contribuyan a la ocurrencia de incidentes significativos de ciberseguridad, conforme a lo establecido en la Ley N° 21.663 y normativa asociada.

10.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.

11	Diciembre 2025	Revisión anual e incorporan aspectos de la Guía Técnica de Seguridad de la Información y Ciberseguridad de apoyo a la norma técnica de Seguridad de la Información y Ciberseguridad de la ley N°21.180, ley de Transformación Digital Versión 1.0 de 23 de marzo 2015.	Ivonne Valdivia / DIVAD; María Waleska Gatica / DIJUR; Marcela Jara / DIFIN; Leonardo Cavieres / DINFO; Carla Toro Pizarro / Depto. de Programación y Control SERVIU Antofagasta; Pedro Mery / Depto. de Programación y Control SERVIU Coquimbo; M. Paula Melis Otonel / Contralora Interna SERVIU Araucanía.

Revisión:	Gabriela Elgueta Poblete/ Subsecretaria de Vivienda y Urbanismo. Vania Navarro Morales/ Encargada de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos, Jefa División de Finanzas Comité de Seguridad de la Información, Ciberseguridad y Gobernanza de Datos Subsecretaría de V. y U. Encargados/as de Seguridad de la Información de SERVIU y Parque Metropolitano de Santiago.
Aprobación:	Carlos Montes Cisternas / Ministro de Vivienda y Urbanismo.

3. ESTABLÉCESE la obligación de 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 efectuar la difusión 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.

4. DÉJASE 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, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.

Ministerio de Vivienda y Urbanismo
Gabinete del Ministro
MINISTRO

CARLOS MONTES CISTERNAS
MINISTRO DE VIVIENDA Y URBANISMO

GEP/CGBM/MPP/DCC/EGY/VNM/MJC/MWGN

DISTRIBUCIÓN:
- Gabinete Ministro V. y U.
- Gabinete Subsecretaria V. y U.
- SEREMI (16)
- Directores/as SERVIU (16)
- Director/a PARQUEMET
- Secretarios/as Regionales Ministeriales de V. y U. (16)
- 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 (CECT)
- Equipo de Estudios Económicos y de Procesos-DIFIN
- Sección Partes y Archivos

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

GABRIELA ELGUETA POBLETE
SUBSECRETARIA DE VIVIENDA Y URBANISMO