

Política General de Seguridad de la Información



	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
	DEPARTAMENTO DE PLANIFICACIÓN SECCIÓN TECNOLOGÍAS DE LA INFORMACIÓN Versión N °9	18 páginas
GESTIÓN DE LA CIBERSEGURIDAD		

Tabla aprobación documento

Actividad	Cargo/Función	Nombre
Modificación/Elaboración	Encargado Titular de Ciberseguridad y Encargado Of. MDA.	Diego García Rojas Patricio Reyes Martínez
Revisión Técnica Nacional	Encargado Oficina Continuidad Operativa y Seguridad	Claudio Henriquez Rebolledo
Revisión Técnica Nacional	Encargado Sección Tecnología de la Información	Víctor Campos Marchant
Revisión Técnica Nacional	Encargada Departamento de Planificación	Carola Salinas Herrera
Metodológica	Gestión de Procesos, Departamento de Planificación	Abigail Espinoza Muñoz
Revisión Normativa	Departamento de Fiscalía y Asesoría Jurídica	Carolina Pérez Díaz
Aprobación	Vicepresidenta/e	Daniela Triviño Millar

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 3 de 18

CONTENIDOS

1. INTRODUCCIÓN.....	5
1.1 Declaración institucional	5
2. OBJETIVO	5
2.1 Objetivos Específicos.....	5
3. ALCANCE	6
4. NORMATIVA Y DOCUMENTOS APLICABLES	6
5. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN	8
6. TERMINOLOGÍA.....	8
7. DESARROLLO DE LA POLÍTICA	10
7.1 Responsabilidades	10
7.1.1 Nivel Estratégico (I Nivel Jerárquico Dirección)	10
7.1.2 Nivel Táctico (II Nivel Jerárquico Gestión y Coordinación)	11
7.1.3 Nivel Operativo (Ejecución)	13
7.2 Gestión de Seguridad de la Información	14
7.3 Gestión de Riesgos	14
7.4 Resumen de los Lineamientos y Controles	14
7.4.1 Organización y Personas	14
7.4.2 Gestión de Activos y Clasificación	15
7.4.3 Control de Acceso e Identidad	15
7.4.4 Protección Tecnológica.....	15
7.4.5 Seguridad Física.....	15
7.4.6 Servicio en la Nube y Proveedores.....	15
7.5 Operador de Importancia Vital (OIV):	15

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 4 de 18

7.6	Continuidad Operacional (BCP) y Recuperación ante Desastres (DRP)	16
7.7	Concientización y Capacitación	16
7.8	Incumplimiento y Sanciones	16
7.9	Protección de la Información	16
7.10	Revisión y Actualización	17
7.11	Aprobación y Vigencia	17
7.12	Difusión y Aceptación	17
8.	ANEXOS.....	18
9.	HISTÓRICO.....	18
9.1	Tabla N°1: Histórico de Modificaciones	18

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 5 de 18

1. INTRODUCCIÓN

1.1 Declaración institucional

La Junta Nacional de Jardines Infantiles (JUNJI) tiene como misión entregar educación parvularia de calidad y bienestar integral a niños y niñas preferentemente entre 0 y 4 años, priorizando a familias en situación de vulnerabilidad socioeconómica, mediante una oferta programática diversa y pertinente a cada contexto territorial.

Para el cumplimiento de esta misión, la información constituye un activo estratégico que debe ser protegido adecuadamente. En este contexto, JUNJI establece la presente **Política General de Seguridad de la Información**, con el propósito de resguardar la **confidencialidad, integridad y disponibilidad** de los activos de información institucionales.

Esta política se enmarca en la normativa vigente del Estado de Chile y en los lineamientos emitidos por la Agencia Nacional de Ciberseguridad (ANCI), adoptando como referencia la **Norma Chilena NCh-ISO/IEC 27001/2023**, orientada a la implementación de un **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en la gestión de riesgos y mejora continua.

Asimismo, la política considera las disposiciones establecidas en la **Ley N°21.663 Marco de Ciberseguridad**, en particular a lo dispuesto en la **Ley N° 19.628** y la **Ley N°21.719 sobre Protección de Datos Personales**, y la **Ley N°20.285 sobre Acceso a la Información Pública**, entre otras normativas aplicables.

JUNJI implementará, mantendrá y mejorará continuamente el Sistema de Gestión de Seguridad de la Información con el propósito de proteger los activos de información de la institución y asegurar la continuidad de los servicios que la institución entrega a la ciudadanía.

La seguridad de la información es responsabilidad de todos los funcionarios/as, colaboradores/as y terceros que se relacionen con la institución, quienes deberán resguardar el adecuado uso y protección de los activos de información institucionales.

2. OBJETIVO

Establecer los lineamientos generales para la gestión y protección de los activos de información de JUNJI, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información institucional, contribuyendo a la continuidad operacional y al cumplimiento de la misión institucional.

2.1 Objetivos Específicos

- Establecer un marco institucional para la gestión de la seguridad de la información y ciberseguridad.
- Cumplir con las leyes, normativas y estándares aplicables en materia de seguridad de la información.
- Identificar y gestionar los activos de información críticos para la operación institucional.
- Implementar procesos de gestión de riesgos de seguridad de la información.
- Diseñar e implementar controles que permitan mitigar riesgos asociados a incidentes de seguridad.
- Promover la concientización y capacitación en seguridad de la información para funcionarios y colaboradores.
- Fortalecer la protección de los datos personales tratados por la institución.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 6 de 18

- Establecer mecanismos para la detección, reporte y gestión de incidentes de seguridad.
- Elaborar y mantener actualizado un inventario de activos de información institucionales asociados a los procesos críticos

3. ALCANCE

La presente política es de cumplimiento obligatorio para:

- Funcionarios de planta y a contrata.
- Personal a honorarios.
- Estudiantes en práctica.
- Proveedores, contratistas y terceros que presten servicios a la institución.

El alcance comprende todos los activos de información utilizados por JUNJI, incluyendo:

- Información en formato digital o físico.
- Sistemas de información.
- Infraestructura tecnológica.
- Redes y plataformas digitales.
- Medios de almacenamiento.
- Información gestionada por proveedores o terceros

Se deberá mantener un inventario actualizado de activos de información relevantes asociados a los procesos críticos, con el fin de sustentar el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP), conforme a las definiciones estratégicas institucionales vigentes (de acuerdo con lo establecido en **"FICHA DE DEFINICIONES ESTRATÉGICAS AÑO 2026 (Anexo Formulario A1)"** (Anexo N°1), seleccionado como primer alcance de implementación.

4. NORMATIVA Y DOCUMENTOS APLICABLES

Leyes

Ley Nro. 17.336 de 1970. [Ministerio de Educación Pública]. Sobre Propiedad Intelectual. Fecha de vigencia a contar del 02 de octubre de 1970.

Ley N°20.285 de 2008. [Ministerio Secretaría General de la Presidencia]. Sobre acceso a la información pública. Fecha vigencia a contar del 20 de agosto 2008.

Ley Nro.21.096 de 2018. [Ministerio Secretaría General de la Presidencia]. Consagra el Derecho a la Protección de los Datos Personales. Fecha vigencia a contar del 16 de junio 2018.

Ley Nro.19.628 de 1999. [Ministerio Secretaría General de la Presidencia]. Sobre Protección de la Vida Privada.

Ley Nro. 21.719 de 2024. [Ministerio Secretaría General de la Presidencia]. Sobre Protección y el tratamiento de los datos personales y con entrada en vigencia conforme a las disposiciones transitorias establecidas en la misma ley."

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 7 de 18

Ley Nro. 21.663 de 2024. [Ministerio del Interior y Seguridad]. Ley Marco sobre Ciberseguridad. Fecha de vigencia a contar 08 de abril 2024.

Decretos

Decreto Supremo N° 1 de 2015. [Ministerio Secretaría General de la Presidencia]. Aprueba Normas Técnicas sobre Sistemas y Sitios WEB de los Órganos de la Administración del Estado.

Decreto Supremo N° 100 de 2005. [Ministerio Secretaría General de la Presidencia]. Fija Texto Refundido, Coordinado y Sistematizado de la Constitución Política de la República de Chile.

Decreto Supremo N° 17 de 2023. [Ministerio Secretaría General de la Presidencia] Establece nueva regulación del Consejo de Auditoría Interna General de Gobierno y Deja sin efecto Decreto N° 12 que indica.

Norma Técnica

Instituto Nacional de Normalización Chile (2013/2023). Norma Chilena Oficial NCH-ISO 27001. Seguridad de la Información Ciberseguridad y Protección de la Privacidad.

Instituto Nacional de Normalización Chile (2017/2022). Norma Chilena Oficial NCH-ISO 27002. Técnicas de Seguridad/Códigos de prácticas para los controles de seguridad de la información.

Resoluciones

Resolución Exenta N° 360 de 2024 Junta Nacional de Jardines Infantiles. Designa a funcionarios que indica como Encargados de Ciberseguridad Titular y Subrogante para la Junta Nacional de Jardines infantiles. Fecha de vigencia a contar 30-04-2024.

Resolución Exenta N° 015/1022 de 2025 Junta Nacional de Jardines Infantiles. Aprueba constitución del Comité Operativo de Seguridad de la Información, de JUNJI. Fecha de vigencia a contar del 22-09-2025.

Resolución Exenta N° 015/1096 de 2025 Junta Nacional de Jardines Infantiles. Aprueba Procedimiento para la Gestión de Perfiles de Navegación y Acceso a Internet, Política de Uso de Correo Electrónico e Internet para la Junta Nacional de Jardines Infantiles. Fecha de vigencia a contar 03-10-2025.

Resolución Exenta N° 015/1496 de 2025 Junta Nacional de Jardines Infantiles. Aprueba Plan de Transformación Digital del Estado, de JUNJI. Fecha de vigencia a contar del 16-12-2025.

Resolución Exenta N° 723 de 2026 Junta Nacional de Jardines Infantiles. Aprueba Política de Privacidad y Términos de uso de los Sitios Web Institucional de la Junta Nacional de Jardines Infantiles. Fecha de vigencia a contar del 04-05-2026.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 8 de 18

5. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de seguridad de la información en JUNJI se basa en los siguientes principios:

Confidencialidad: La información debe ser accesible únicamente por personas autorizadas.

Privacidad: El tratamiento de los datos personales debe realizarse conforme a la normativa vigente en materia de protección de datos personales.

Integridad: La información debe mantenerse completa, exacta y protegida contra modificaciones no autorizadas.

Disponibilidad: La información y los sistemas que la procesan deben estar disponibles cuando sean requeridos para el cumplimiento de las funciones institucionales.

Gestión de riesgos: La seguridad de la información debe gestionarse mediante la identificación, análisis, evaluación y tratamiento de riesgos.

Continuidad y resiliencia: La institución debe mantener capacidades de preparación, respuesta y recuperación frente a eventos de contingencia que afecten la continuidad operacional.

Mejora continua: El SGSI debe fortalecerse continuamente mediante la planificación, ejecución, verificación y mejora de sus procesos y controles.

Cumplimiento normativo: La gestión de seguridad de la información debe realizarse en conformidad con la normativa legal, regulatoria, contractual y de transparencia aplicable.

Responsabilidad: Todos los funcionarios y colaboradores deben proteger la información y los recursos tecnológicos institucionales, y cumplir las políticas y procedimientos de seguridad de la información.

6. TERMINOLOGÍA

- **Amenaza:** Evento potencial que puede causar daño a un activo de información.
- **Vulnerabilidad:** Debilidad que puede ser explotada por una amenaza.
- **Riesgo:** Probabilidad de que una amenaza explote una vulnerabilidad y genere un impacto.
- **Evento de Seguridad:** Suceso que puede derivar en un incidente.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Control:** Medida que reduce un riesgo.
- **Clasificación de la Información:** Proceso de categorización según sensibilidad.
- **Datos Personales:** Información relativa a una persona natural identificada o identificable.
- **Brecha de Seguridad:** Incidente que afecta datos personales.
- **Autenticación:** Proceso de verificación de identidad.
- **Autorización:** Proceso de asignación de permisos.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 9 de 18

- **Cifrado:** Técnica para proteger información mediante codificación.
- **BCP:** Plan de continuidad operacional.
- **DRP:** Plan de recuperación ante desastres.
- **RTO:** Tiempo máximo para recuperar un servicio.
- **RPO:** Punto máximo de pérdida de datos aceptable.
- **Seguridad de la Información:** Protección de información garantizando confidencialidad, disponibilidad e integridad.
- **Ciberseguridad:** Protección de sistemas, redes y datos frente a amenazas digitales.
- **Activos de Información:** Información, sistemas, infraestructura tecnológica y otros recursos necesarios para el tratamiento y resguardo de la información institucional
- **Propietario del Activo:** Funcionario/a, jefatura o unidad responsable de la gestión, clasificación, resguardo y uso adecuado de un activo de información, incluyendo la definición de niveles de acceso, criticidad y requerimientos de protección.
- **Custodio del Activo:** Funcionario/a, unidad o tercero responsable de la administración operativa, mantenimiento, almacenamiento, respaldo o protección técnica y física de un activo de información, conforme a los lineamientos definidos por el propietario del activo.
- **Política:** Conjunto de reglas declaradas por la institución.
- **Proceso:** Actividades que transforman entradas en resultados.
- **Sistemas:** Plataformas y software que procesan información.
- **Infraestructura:** Base física o virtual que soporta sistemas e información.
- **Área Segura:** Espacios físicos que contienen información sensible.
- **Servicio Esencial:** Servicio crítico provisto por organismos públicos.
- **Encargado/a de Seguridad de la Información:** Responsable de supervisar cumplimiento de políticas.
- **Encargado/a Titular de Ciberseguridad:** Asesora sobre ciberseguridad a nivel institucional y nacional.
- **Analista de Ciberseguridad:** Implementa controles, protocolos de respuesta y reporta incidentes.
- **DPO:** Responsable de protección de datos personales.
- **Funcionarios:** Personal de planta, contrata, honorarios, reemplazos y suplencias.
- **Alumno/a en práctica:** Persona en práctica académica, sujeta a las mismas políticas.
- **Proveedores / Terceros:** Entidades externas que prestan servicios a JUNJI.
- **Comité Operativo de Seguridad de la Información:** Supervisa políticas y procedimientos de seguridad.
- **CSIRT:** Equipo de respuesta ante incidentes informáticos del Gobierno de Chile.
- **ANCI:** Agencia Nacional de Ciberseguridad.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 10 de 18

- **Incidente de Seguridad:** Evento que compromete la información.
- **Incidente de efecto significativo:** Evento que afecta servicios esenciales, integridad o datos personales.
- **Administración de Riesgos:** Gestión de riesgos de seguridad de la información.
- **Evaluación de Riesgos:** Identificación de amenazas y vulnerabilidades y su impacto.
- **OIV (Operador de Importancia Vital):** Entidad pública o privada que presta servicios esenciales para el país, cuya interrupción o falla podría afectar gravemente la seguridad, economía o bienestar de la nación. Los OIV deben cumplir estándares de ciberseguridad, implementar medidas de protección, designar un delegado de ciberseguridad y reportar incidentes al CSIRT Nacional, en conformidad con la Ley N°21.663 y supervisión de la ANCI.

7. DESARROLLO DE LA POLÍTICA

7.1 Responsabilidades

La gestión de la seguridad de la información se organiza en tres niveles:

Nivel Estratégico

- Vicepresidenta/e Ejecutiva/o
- Comité Operativo de Seguridad

Nivel Táctico

- Directores/as Regionales
- Directores/as Departamentos
- Sección Gobernanza de Datos
- Sección de Tecnología de la Información
- Oficina Continuidad Operativa y Seguridad de la Información
- Encargado/a Titular de Ciberseguridad
- Encargado/a de Seguridad de la Información

Nivel Operativo

- Cada activo de información deberá tener formalmente definido un propietario y cuando corresponda, un custodio.
- Usuarios
- Proveedores

7.1.1 Nivel Estratégico (I Nivel Jerárquico Dirección)

Vicepresidenta(e) Ejecutiva(o)

- Establecer la Política de Seguridad de la Información institucional.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 11 de 18

- Definir los roles y responsabilidades en materia de seguridad de la información.
- Designar a los miembros del Comité de Seguridad de la Información, al Encargado de Seguridad de la Información y al Encargado Titular de Ciberseguridad, mediante el acto administrativo correspondiente.
- Autorizar la publicación y difusión de la Política General de Seguridad de la Información.
- Asignar recursos al Sistema de Gestión de Seguridad de la Información (SGSI) en todas sus fases.
- Asignar recursos para mejoras en ciberseguridad.
- Autorizar la gestión de claves institucionales.

Comité Operativo de Seguridad de la Información

- Supervisar la implementación de la Política de Seguridad de la Información.
- Evaluar el estado de la seguridad de la información institucional.
- Proponer medidas de mejora en seguridad de la información y ciberseguridad.
- Monitorear el avance de las estrategias de control y tratamiento de riesgos.
- Coordinar la gestión institucional frente a incidentes relevantes.

7.1.2 Nivel Táctico (II Nivel Jerárquico Gestión y Coordinación)

Directores/as Regionales

- Promover la Política de Seguridad de la Información y Ciberseguridad.
- Supervisar su cumplimiento en el nivel regional.
- Autorizar claves en su ámbito de responsabilidad.

Director/a Departamento de Gestión y Desarrollo de Personas

- Velar por el cumplimiento del artículo 61 letra h) del DFL N°29 (Estatuto Administrativo) respecto a confidencialidad de la información.
- Incorporar la seguridad de la información en los procesos de inducción institucional.
- Incluir capacitación anual en seguridad de la información y ciberseguridad.
- Entregar material institucional sobre la política de seguridad.
- Gestionar la aceptación formal de las políticas por parte de los funcionarios.
- Autorizar claves cuando corresponda.

Director/a Departamento de Planificación

Encargado/a Sección Gobernanza de Datos

- Gestionar, a través del Encargado de Seguridad de la Información, los cambios a las políticas de seguridad de la información.
- Supervisar el correcto uso y gobernanza de los datos institucionales.

Encargado/a Sección Tecnologías de la Información

- Coordinar con la Oficina de Continuidad Operativa y Seguridad de la Información la mitigación de riesgos que puedan afectar la plataforma tecnológica:

- ✓ Comunicaciones

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 12 de 18

- ✓ Datacenter
 - ✓ Servicios cloud
 - ✓ Servicios de seguridad
 - ✓ Firma electrónica y certificados digitales
 - ✓ Sitios web institucionales
- Gestionar la adopción de estándares tecnológicos institucionales.
 - Autorizar claves de acceso en coordinación con las políticas vigentes

Encargado/a Oficina de Continuidad Operativa y Seguridad de la Información

- Coordinar gestión de seguridad y continuidad operativa.
- Supervisar implementación de controles y planes de contingencia.
- Mantener enlace con Encargados de Ciberseguridad y Seguridad.
- Aprobar planes de acción y reportes, incluyendo OIV.
- Participar en BCP y DRP institucionales.

1. Encargado/a Titular de Ciberseguridad

- Coordinar el desarrollo inicial de las políticas de seguridad al interior de la institución.
- Controlar su implementación y velar por su correcta aplicación.
- Aprobar controles de seguridad en la plataforma tecnológica.
- Administrar el ciclo de vida de políticas, procedimientos y estándares de ciberseguridad.
- Participar activamente en el Comité Operativo de Seguridad de la Información y priorización de incidentes.
- Coordinar la priorización y respuesta ante incidentes de seguridad.
- Administrar inventario de activos críticos y vulnerabilidades.
- Implementar medidas de protección tecnológica (firewalls, cifrado, IDS).
- Mantener enlace con encargados de ciberseguridad de otros organismos públicos.
- Ejecutar acciones para resguardar a la institución frente a incidentes de seguridad.
- Aprobar procedimientos y políticas específicas derivados de la política general.
- Elaborar el plan de sanciones junto al Encargado de Seguridad de la Información.
- Reportar incidentes, vulnerabilidades y oportunidades de mejora conforme al protocolo institucional de gestión y escalamiento de incidentes, respetando estrictamente la estructura jerárquica y el conducto regular definido para nivel central y Direcciones Regionales.
- Gestionar incidentes tecnológicos y reportes a ANCI.
- Elaborar el Plan de Recuperación ante Desastres (DRP).

2. Encargado/a de Seguridad de la Información

- Supervisar seguridad física y acceso a recursos críticos.
- Coordinar con Ciberseguridad para protección integral.
- Elaborar planes de continuidad y recuperación ante desastres.
- Aprobar controles de seguridad física e infraestructura tecnológica.
- Elaborar, junto a Ciberseguridad, plan de sanciones y procedimientos.
- Desarrollar el Plan de Continuidad de Negocio (BCP) institucional.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 13 de 18

Directores/as Departamentos

- Difundir políticas específicas y procedimientos de seguridad.
- Supervisar su cumplimiento dentro de sus unidades.
- Autorizar claves según competencias.

7.1.3 Nivel Operativo (Ejecución)

Responsables de la Información

Cada **Director/a de Departamento, Jefatura de Sección, Unidad y Oficina** o quien éste designe, debe:

- Garantizar la protección y uso adecuado de la información bajo su responsabilidad.
- Clasificar, custodiar y mantener actualizada la información.
- Aplicar la clasificación de la Información institucional:
 1. Pública
 2. Uso Interno
 3. Confidencial
 4. Reservada o Secreta

Usuarios de la Información (Funcionarios/as)

Cada **funcionario/a** que acceda, procese o gestione información institucional, debe:

- Cumplir con las políticas y procedimientos de seguridad de la información.
- Utilizar los recursos tecnológicos de forma responsable.
- Acceder únicamente a la información autorizada.
- Utilizar exclusivamente herramientas tecnológicas autorizadas por JUNJI.
- Reportar incidentes o vulnerabilidades a través de la **Mesa de Ayuda (MDA)**.

Principales responsabilidades:

- Usar la información sólo para fines autorizados.
- Conocer y respetar las políticas institucionales de seguridad.
- Evitar la divulgación o uso no autorizado de información.
- Reportar incidentes de seguridad en el canal formal definido por la Institución.

Proveedores

Todo **proveedor o tercero** que acceda o gestione información institucional de JUNJI, debe:

- Cumplir con la Política General de Seguridad de la Información de JUNJI.
- Cumplir con políticas y procedimientos del SGSI.
- Gestionar riesgos asociados a servicios prestados a JUNJI incluyendo, pero no limitado a:
 - Comunicaciones
 - Datacenter
 - Servicios cloud

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 14 de 18

- Firma electrónica
- Certificados digitales
- Infraestructura tecnológica

7.2 Gestión de Seguridad de la Información

La JUNJI implementará un **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en la norma **NCh-ISO/IEC 27001:2023**, orientado a la gestión de riesgos y mejora continua.

Este sistema contemplará, entre otros aspectos:

- Identificación y clasificación de activos de información.
- Evaluación y tratamiento de riesgos de seguridad.
- Implementación de controles de seguridad.
- Gestión de incidentes de seguridad.
- Gestión de continuidad operativa.
- Concientización y capacitación en seguridad de la información.
- Monitoreo y revisión continua de los controles implementados.

El Sistema de Gestión de Seguridad de la Información será monitoreado y evaluado mediante indicadores de desempeño, auditorías internas y revisiones periódicas por la Alta Dirección, con el fin de asegurar su eficacia y mejora continua.

7.3 Gestión de Riesgos

JUNJI realizará evaluaciones de riesgos periódicas a través de un proceso formal de gestión de riesgos de seguridad de la información que permita identificar, analizar, evaluar y tratar los riesgos asociados a los activos de información institucionales.

El tratamiento de riesgos podrá considerar las siguientes estrategias:

- Mitigar el riesgo
- Transferir el riesgo
- Evitar el riesgo
- Aceptar el riesgo

Los incidentes de seguridad de la información deberán ser registrados, clasificados según su criticidad y gestionados conforme a procedimientos definidos, incluyendo su análisis, respuesta y generación de acciones de mejora.

7.4 Resumen de los Lineamientos y Controles

La implementación se regirá por políticas específicas y controles de la NCh-ISO/IEC 27001:2023, incluyendo:

7.4.1 Organización y Personas

- Políticas de seguridad (A.5.1)
- Roles y responsabilidades (A.5.2)

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 15 de 18

- Concientización y capacitación (A.6.3)
- Términos y condiciones (A.6.2)
- Proceso disciplinario (A.6.4)
- Trabajo a distancia (A.6.7)
- Escritorio y pantalla despejada (A.7.7)

7.4.2 Gestión de Activos y Clasificación

- Inventario de activos (A.5.9)
- Propiedad intelectual (A.5.32)
- Clasificación y manejo de la información en dos categorías:
 - Confidencial (reservada y secreta).
 - Pública.
 - La Matriz de Clasificación definirá criterios, ejemplos y salvaguardas.

7.4.3 Control de Acceso e Identidad

- Autenticación segura (A.8.5)
- Gestión de cuentas y privilegios (A.8.2, A.8.3)

7.4.4 Protección Tecnológica

- Gestión de vulnerabilidades y parches; antimalware (A.8.7); configuraciones seguras.
- Cifrado (A.8.24) en tránsito y en reposo según sensibilidad.
- Respaldo (A.8.13), pruebas de restauración, retención y supresión (A.8.10).
- Monitoreo y registros (A.8.16), correlación de eventos y alertas.
- Filtro web (A.8.23) y segmentación de red.
- Gestión de cambios y entornos separados dev/test/prod (A.8.31).
- Desarrollo seguro (A.8.28)
- Desarrollo externo (A.8.30).

7.4.5 Seguridad Física

- Perímetros y acceso físico (A.7.1, A.7.2)
- Medios de almacenamiento (A.7.10)
- Eliminación segura o reutilización de equipos (A.7.14)

7.4.6 Servicio en la Nube y Proveedores

- Seguridad para uso de servicios en la nube (A.5.23).
- Gestión de proveedores (A.5.19, A.5.22), evaluaciones, SLA/ANS y cláusulas de seguridad y privacidad.

7.5 Operador de Importancia Vital (OIV):

- Reporte de incidentes críticos al CSIRT Nacional: 24 horas si afecta servicios esenciales.
- Plan de acción: **7 días** desde conocimiento del incidente.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 16 de 18

- Informe final: **15 días corridos**; si no está resuelto, informes parciales hasta resolución.
- Contenido mínimo de reportes: identificación de institución, datos del Encargado Titular de Ciberseguridad, fecha/hora del incidente, evidencias, repercusiones, taxonomía según ANCI.
- Canales de reporte: portal ANCI (clave única), teléfono 1510, correo ayuda@anci.gob.cl.
- Sanciones por incumplimiento: hasta 10.000 UTM (Servicios Esenciales) y hasta 20.000–40.000 UTM (OIV) según Ley 21.663.

7.6 Continuidad Operacional (BCP) y Recuperación ante Desastres (DRP)

- JUNJI mantendrá **BCP** institucional (liderado por el ESI) y **DRP** de TI (liderado por Ciberseguridad) para asegurar la **disponibilidad** de servicios críticos.
- Se definirán RTO/RPO, escenarios de contingencia, prioridades de recuperación y pruebas periódicas documentadas (A.5.35–A.5.37).
- Los resultados de pruebas generarán planes de mejora.

7.7 Concientización y Capacitación

- Programa **anual y obligatorio** de sensibilización y formación en seguridad de la información, ciberseguridad y protección de datos, con métricas de participación y eficacia.
- Inducción para ingresos, refuerzos temáticos y campañas de phishing simulado (cuando aplique).

7.8 Incumplimiento y Sanciones

- El **incumplimiento** de esta política, políticas específicas, procedimientos o contratos será sancionado conforme a su **gravedad** y al **Estatuto Administrativo**.
- En el caso de **proveedores/terceros**, podrá implicar **término anticipado de contrato** y responsabilidades civiles/penales, sin perjuicio de las acciones administrativas, civiles o penales que correspondan.
- El **Comité Operativo de Seguridad de la Información** podrá iniciar procedimientos de oficio o por denuncia, resguardando debido proceso y proporcionalidad.

7.9 Protección de la Información

- JUNJI tratará datos personales conforme a la **Ley 19.628 y 21.719** y principios de **licitud, lealtad, transparencia, minimización, exactitud y limitación del plazo de conservación**.
- Se implementarán **medidas técnicas y organizativas** proporcionales al riesgo (cifrado, control de acceso, registros, auditorías, evaluación de impacto en protección de datos cuando aplique).
- Se resguardarán los **derechos de los titulares** (acceso, rectificación, portabilidad, supresión, oposición, entre otros), habilitando **canales y plazos** para su atención.
- Ante **brechas de seguridad** que afecten datos personales, se **notificará** a los afectados y a la **Agencia de Protección de Datos Personales**, según plazos y requisitos legales.
- Los **encargos de tratamiento** con terceros se formalizarán mediante acuerdos que establezcan obligaciones de seguridad y privacidad, y la sujeción a auditorías.
- Se incorporan controles técnicos de alto nivel alineados con NCh-ISO/IEC 27001:2023 y buenas prácticas actuales de ciberseguridad:

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 17 de 18

- ✓ **Gestión y retención de registros (logs):** Los sistemas críticos deberán generar, resguardar y monitorear registros de actividad que permitan la trazabilidad de accesos, eventos de seguridad, modificaciones relevantes y detección de incidentes.
- ✓ **Autenticación Multifactor (MFA):** JUNJI promoverá el uso de mecanismos de autenticación Multifactor para el acceso a sistemas críticos, servicios remotos, plataformas en la nube y cuentas con privilegios elevados.
- ✓ **Segregación de funciones:** Se establecerán controles que permitan separar funciones incompatibles o críticas, con el fin de reducir riesgos de error, fraude, alteración no autorizada o uso indebido de privilegios.
- ✓ **Revisión periódica de accesos y privilegios:** Los accesos a sistemas y plataformas institucionales deberán ser revisados periódicamente para asegurar que los permisos asignados sean consistentes con las funciones y responsabilidades vigentes de cada usuario.
- ✓ **Gestión de respaldos seguros:** Los respaldos de información crítica deberán considerar mecanismos de protección adecuados, incluyendo almacenamiento seguro, pruebas de restauración y, cuando corresponda, respaldos offline o inmutables para mitigar riesgos de Ransomware u otras amenazas.
- ✓ **Gestión de servicios en la nube y terceros tecnológicos:** Los servicios cloud y proveedores tecnológicos deberán cumplir requisitos de seguridad de la información, continuidad operativa, protección de datos personales y controles contractuales acordes a los riesgos asociados.

7.10 Revisión y Actualización

- Esta política será revisada **al menos una vez al año** o ante cambios relevantes (legales/regulatorios, tecnológicos, de riesgo, organizacionales o instrucción de autoridad).
- Las actualizaciones serán aprobadas por el **Comité Operativo** y promulgadas por la **Vicepresidencia Ejecutiva**.

7.11 Aprobación y Vigencia

Esta política ha sido **aprobada** por el **Comité Operativo de Seguridad de la Información** y el/la **Encargado/a Titular de Ciberseguridad**, y es **promulgada** por la **Vicepresidencia Ejecutiva**.

Entra en vigencia a partir de la emisión del acto administrativo correspondiente.

En caso de conflicto entre esta política y normas legales o reglamentarias vigentes, prevalecerán estas últimas.

7.12 Difusión y Aceptación

Será difundida mediante los canales institucionales oficiales.

Su aceptación será obligatoria, registrando evidencia de conocimiento y conformidad.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	PL-TIC-003
		Versión N°9
		Página 18 de 18

8. ANEXOS

Al presente documento se adjuntan los siguientes Anexos:

- PL-TIC-003-A1 Anexo N°1: "FICHA DE DEFINICIONES ESTRATÉGICAS AÑO 2026-2026 (Formulario A1)"

9. HISTÓRICO

9.1 Tabla N°1: Histórico de Modificaciones

Resumen de Modificaciones						
N°	Versión Vigente	Versión Actualizada	Fecha (Mes/Año)	Título	Subtitulo	Descripción Modificación
1	8		21-11-2019			Este documento modifica, reemplaza y deja sin efecto la Política General de la Seguridad de la Información, en su séptima versión aprobado según Resolución Exenta Nro.017/0524 del 27 de agosto de 2019.
2	9		01-08-2025			Este documento modifica, reemplaza y deja sin efecto la Política General de la Seguridad de la Información, en su octava versión aprobada según Resolución Exenta Nro.015/0757 del 21 de noviembre de 2019.