

POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS



JUNJI
Ministerio de
Educación

Gobierno de Chile

VERSIÓN N.º 1

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
	DEPARTAMENTO DE PLANIFICACIÓN SECCIÓN TECNOLOGÍAS DE LA INFORMACIÓN Versión N.º 1	11 páginas
GESTIÓN DE LA CIBERSEGURIDAD		

TABLA DE APROBACIÓN DEL DOCUMENTO

Actividad	Cargo/Función	Nombre
Modificación/Elaboración	Encargado de Ciberseguridad, Sección Tecnologías de la Información, Departamento de Planificación	Diego García Rojas
Revisión Técnica Nacional	Encargado Oficina Continuidad Operativa y Seguridad, Sección Tecnologías de la Información, Departamento de Planificación	Claudio Henríquez Rebolledo
Revisión Técnica Nacional	Encargado Sección Tecnología de la Información, Departamento de Planificación	Víctor Campos Marchant
Revisión Técnica Nacional	Encargada Departamento de Planificación	Carola Salinas Herrera
Metodológica	Jefe Oficina de Gestión de Procesos, Sección de Gestión estratégica, Departamento de Planificación	Richard Llinima Sandoval
Revisión Normativa	Directora (S) Departamento de Fiscalía y Asesoría Jurídica	María Elisa Peralta Acevedo
Aprobación	Vicepresidenta Ejecutiva (S)	Denise Alejandra Arriagada Obregón

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 1 de 11

CONTENIDOS

1	INTRODUCCIÓN	2
2	OBJETIVO	2
3	ALCANCE	3
4	NORMATIVA Y DOCUMENTOS APLICABLES	3
5	TERMINOLOGÍA	4
6	DESARROLLO DE LA POLÍTICA	5
6.1	Principios Rectores	5
6.2	Responsabilidades	5
6.3	Directrices de Configuración del Endpoint.....	8
6.4	Gestión, Aplicación y Cumplimiento de la Política de Ciberseguridad	9
7	ANEXOS.....	11
8	HISTÓRICO	11

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 2 de 11

1 INTRODUCCIÓN

La Junta Nacional de Jardines Infantiles (JUNJI), en el marco de su Sistema de Gestión de Seguridad de la Información (SGSI) y conforme a las exigencias establecidas en la Ley N.º 21.663, Ley Marco sobre Ciberseguridad, reconoce que los dispositivos finales institucionales constituyen uno de los principales vectores de riesgo para la confidencialidad, integridad y disponibilidad de la información institucional.

En consideración al tratamiento de datos personales y datos sensibles asociados a niños, niñas, funcionarios y funcionarias y terceros relacionados con la institución, la presente política establece lineamientos de seguridad para dispositivos finales (endpoints), bajo un enfoque de defensa en profundidad y confianza cero (Zero Trust), orientado a reducir riesgos de ciberseguridad, fortalecer la continuidad operacional y resguardar los activos de información institucionales.

Las medidas definidas en este instrumento buscan establecer controles preventivos, detectivos y correctivos sobre el uso de estaciones de trabajo, computadores portátiles y demás dispositivos autorizados por JUNJI, promoviendo el uso seguro de plataformas institucionales y servicios en la nube autorizados.

2 OBJETIVO

Establecer los principios rectores, lineamientos normativos, administrativos y técnicos para la protección de los dispositivos finales (endpoints) institucionales de JUNJI, con el propósito de reducir riesgos asociados a incidentes de ciberseguridad, fuga de información, software no autorizado y uso indebido de recursos tecnológicos institucionales, resguardando la confidencialidad, integridad y disponibilidad de la información institucional conforme al marco normativo vigente.

2.1 Objetivos específicos

- Implementar controles de seguridad sobre interfaces físicas y lógicas de los dispositivos institucionales, incluyendo puertos USB y conectividad Bluetooth, con el fin de reducir riesgos asociados a malware, dispositivos no autorizados y extracción indebida de información.
- Restringir la utilización de dispositivos personales o no autorizados que permitan transferencia de información hacia o desde la red institucional.
- Promover el uso de plataformas institucionales autorizadas para almacenamiento, respaldo y compartición de información, privilegiando servicios corporativos en la nube definidos por JUNJI.
- Implementar controles de prevención de fuga de información (DLP) mediante herramientas de monitoreo y protección institucionalmente autorizadas.
- Fortalecer la trazabilidad y monitoreo de eventos asociados al uso de activos tecnológicos institucionales, conforme a las facultades legales y administrativas vigentes.
- Establecer mecanismos formales para la autorización excepcional de accesos, dispositivos o software restringido, garantizando trazabilidad, temporalidad y evaluación de riesgos.
- Contribuir al cumplimiento de la Ley N.º 21.663, la Ley N.º 21.719 y demás normativa aplicable en materia de seguridad de la información y protección de datos personales.

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 3 de 11

3 ALCANCE

Esta política y las asociadas a esta son de cumplimiento obligatorio para todos los funcionarios y funcionarias de planta, a contrata, honorarios y estudiantes en práctica que cumplan funciones tanto en oficinas como en jardines y a todo el personal externo que preste servicios profesionales y utilice los servicios de red, sistemas o mensajería institucionales y que tenga acceso a información de JUNJI que pueda afectar sus recursos informáticos. Esta política contempla los siguientes controles definidos en la norma NCh-ISO 27001:2023:

Control 5.10 "Uso aceptable de información y otros activos asociados"

Control 5.14 "Transferencia de información"

Control 5.23 "Seguridad de la información para uso de servicio en la nube"

Control 7.10 "Medios de almacenamiento"

Control 8.7 "Protección contra malware"

Control 8.16 "Actividades de monitoreo"

Control 8.23 "Filtro web"

4 NORMATIVA Y DOCUMENTOS APLICABLES

Normativa

Ley N.º20.285 de 2008. [Ministerio Secretaría General de la Presidencia]. Sobre acceso a la información pública. Fecha de vigencia a contar del 20 de agosto de 2008.

Ley N.º 17.336 de 1970. [Ministerio de Educación Pública]. Sobre Propiedad Intelectual. Fecha de vigencia a contar del 2 de octubre de 1970.

Ley N.º 21.719 de 2024. [Ministerio Secretaría General de la Presidencia]. Sobre Protección y el tratamiento de los datos personales. Fecha vigencia a contar 13 diciembre del 2024, con fecha diferida de vigencia a contar de 1 de diciembre de 2026.

Ley N.º 21.663 de 2024. [Ministerio del Interior y Seguridad]. Ley Marco sobre Ciberseguridad. Fecha de vigencia a contar de 8 de abril de 2024.

Resoluciones Exentas

Resolución Exenta N.º 015/863 (2024), Aprueba el Manual de Procedimientos para la Formulación, Estructura y Control de Documentos Procedimentales de JUNJI (25 de octubre de 2024).

Resolución Exenta N.º 015/429 (2025), Establece la nueva organización interna de JUNJI, tanto a nivel nacional como regional (2 de mayo de 2025)

Resolución Exenta N.º 831 (2026) [Junta Nacional de Jardines Infantiles], Deja sin efecto la Resolución Exenta N.º 015/0757, de fecha 21 de noviembre de 2019, de la Vicepresidenta Ejecutiva de la Junta Nacional de Jardines Infantiles, que dejó sin efecto la Resolución Exenta N.º 015/0524, de fecha 27 de agosto de 2019 y que "Aprueba Política General de Seguridad de la información, de la Junta Nacional de Jardines Infantiles, Novena Versión".

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 4 de 11

Norma Técnica

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

Instituto Nacional de Normalización Chile (2017/2022). Norma Chilena Oficial NCh-ISO 27002:2025. Técnicas de Seguridad/Códigos de prácticas para los controles de seguridad de la información.

Reglamento (UE) 2016/679. Reglamento General de Protección de Datos. Como referencia internacional de buenas prácticas es importante considerar los Principios del Reglamento General de Protección de Datos (GDPR) de la UE en cuanto a la "Privacidad desde el Diseño" y la "Seguridad por Defecto", asegurando que los dispositivos terminales minimicen la exposición de datos sensibles.

Normativa Interna de la Junta Nacional de Jardines Infantiles de la Política de Control de Acceso Lógico.

5 TERMINOLOGÍA

Seguridad de la Información: Conjunto de prácticas y mecanismos implementados por una institución y sus sistemas tecnológicos para proteger la información, garantizando su confidencialidad, disponibilidad e integridad en todo momento.

Ciberseguridad: Área enfocada en la protección de sistemas, redes y datos frente a amenazas digitales. Incluye técnicas, herramientas y procesos que resguardan la integridad y funcionamiento de programas, dispositivos y redes, con el fin de reducir riesgos asociados a la información digital y prevenir accesos no autorizados o interrupciones en las operaciones.

Endpoint (Punto final): Es cualquier dispositivo físico o virtual que se conecta a una red. En ciberseguridad, se refiere específicamente a los equipos de los usuarios finales y los servidores donde se instala un agente o sensor de XDR para recopilar telemetría y bloquear amenazas de forma centralizada.

Incidente de Seguridad: Suceso o serie de eventos no planificados que afectan la seguridad de la información o ciberseguridad, con el potencial de comprometer las operaciones de una organización y poner en riesgo sus datos y sistemas.

Activo de Información: Recursos informáticos considerados valiosos o críticos para una institución, ya que son esenciales para su funcionamiento y el cumplimiento de sus objetivos estratégicos.

Sistema de Gestión de Seguridad de la Información (SGSI): Marco de trabajo estructurado que permite a una organización establecer, implementar, mantener y mejorar continuamente la seguridad de su información, asegurando el logro de sus metas operativas y de servicio.

OneDrive: Plataforma de almacenamiento en la nube que permite guardar, compartir y acceder a archivos y documentos desde cualquier dispositivo con conexión a Internet, utilizando la cuenta institucional de JUNJI.

SharePoint de JUNJI: Herramienta colaborativa basada en la nube que facilita la gestión, organización, compartición de documentos y recursos institucionales. Permite a los equipos trabajar de manera coordinada, acceder a información centralizada y mejorar la eficiencia en los procesos internos.

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 5 de 11

Correo Masivo: Envío de un mensaje electrónico a un número de destinatarios que excede el límite estándar establecido por la plataforma de correo institucional.

Autenticación Multifactor (MFA): Método de seguridad que añade capas adicionales de verificación al proceso de inicio de sesión, requiriendo múltiples formas de autenticación para acceder a sistemas o plataformas.

Mailing: Estrategia de comunicación digital que implica el envío masivo de correos electrónicos a una lista de contactos, con el objetivo de transmitir información relevante o mantener una comunicación efectiva con funcionarios y funcionarias, usuarios, proveedores y audiencias institucionales.

6 DESARROLLO DE LA POLÍTICA

6.1 Principios Rectores

La presente política se regirá por los siguientes principios:

a) Principio de Mínimo Privilegio

Los accesos y permisos sobre los recursos tecnológicos institucionales deberán otorgarse únicamente en la medida necesaria para el cumplimiento de las funciones laborales autorizadas.

b) Principio de Defensa en Profundidad

La seguridad institucional deberá implementarse mediante múltiples capas de control preventivo, detectivo y correctivo, reduciendo la dependencia de un único mecanismo de protección.

c) Principio de Confianza Cero (Zero Trust)

Todo dispositivo, usuario, aplicación o conexión deberá ser validado y autorizado explícitamente antes de acceder a recursos institucionales.

d) Principio de Proporcionalidad

Las medidas de monitoreo y control tecnológico deberán ser proporcionales al riesgo identificado y orientadas exclusivamente a la protección de los activos institucionales y cumplimiento normativo.

e) Principio de Trazabilidad

Toda excepción, acceso privilegiado, evento de seguridad o actividad relevante sobre los activos tecnológicos institucionales deberá contar con mecanismos de registro y auditoría.

f) Principio de Protección de Datos

Las medidas de seguridad deberán resguardar especialmente la información personal y sensible tratada por JUNJI, conforme a la normativa vigente.

6.2 Responsabilidades

Directores/as de Departamentos y Directores/as Regionales de JUNJI.

- Supervisar que el personal bajo su cargo cumpla con las disposiciones establecidas en esta política.
- Autorizar las solicitudes de acceso especiales para los endpoints que se encuentren bloqueados, mediante los formularios correspondientes.
- Garantizar que el personal a su cargo utilice de manera adecuada los endpoints fiscales.

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 6 de 11

Encargado/a Sección de Tecnología de la Información, Departamento de Planificación

- Servir como punto de contacto para brindar orientación, asesoría, actualizaciones y solución de problemas relacionados con los permisos especiales para el endpoint.
- Proponer y ejecutar configuraciones de seguridad en los sistemas informáticos y servicios asociados a los endpoints.
- Instalar y mantener las aplicaciones autorizadas para su uso institucional.
- Desinstalar las aplicaciones no autorizadas para su uso institucional.
- Deshabilitar el acceso a recursos institucionales que sean utilizados de manera inapropiada.
- Bloquear sitios web o servicios en línea que representen un riesgo para la seguridad, afecten el rendimiento de la red o no estén relacionados con las funciones institucionales.
- Implementar medidas de seguridad y prevención en la red institucional para garantizar la continuidad, integridad y disponibilidad de los sistemas.
- Gestionar y administrar en planilla digital las excepciones autorizadas en los endpoints.
- Aislar la red de visitas de los recursos internos de JUNJI para proteger la integridad y seguridad de la información institucional.
- Aprobar en conjunto con el Encargado/a de Ciberseguridad las aplicaciones o software que puedan ser instalados en la institución.
- Aprobar en conjunto con el Encargado/a de Ciberseguridad los medios masivos dentro de la red JUNJI.

Encargado/a de Ciberseguridad, Sección de Tecnología de la Información, Departamento de Planificación

- Velar por la difusión y cumplimiento efectivo de la presente política en toda la institución.
- Monitorear el funcionamiento y operación adecuada de los sistemas informáticos y servicios relacionados con los endpoints.
- Garantizar la correcta aplicación de la política y brindar apoyo a las oficinas técnicas responsables de la administración y gestión del uso o excepciones en los endpoints.
- Aprobar, en coordinación con la Jefatura de la Sección de Tecnologías de la Información, las aplicaciones autorizadas para su instalación en los equipos institucionales.
- Bloquear dispositivos y aplicaciones que representen un riesgo para la seguridad, afecten el rendimiento de la red o no estén alineados con las actividades propias de la institución o sus funcionarios y funcionarias.
- Implementar medidas de seguridad y prevención en la red institucional para asegurar la continuidad, integridad y disponibilidad de los sistemas y de los servicios de red.
- Controlar planilla de dispositivos y aplicaciones autorizadas en la red institucional.
- Evaluar y autorizar o rechazar solicitudes de excepciones en los endpoints, según corresponda.
- Asesorar y revisar la seguridad de la información que deba ser compartida con terceros externos a la institución, especialmente cuando el personal de JUNJI manifieste dudas al respecto.
- Actualizar periódicamente la presente política, con el objetivo de asegurar su idoneidad, eficiencia y efectividad continua en el tiempo.

Encargado/a Oficina Mesa de Ayuda (MDA) y/u Oficina de Continuidad Operativa, Sección de Tecnología de la Información, Departamento de Planificación

- Instalar agente de antivirus en los equipos de JUNJI.
- Monitorear estado del antivirus en cada equipo de DIRNAC
- Revisión de medios externos (pendrive y/o disco duro externo) que no contengan malware.
- Actividades que sean encomendadas por el Encargado de la Sección de TI.

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 7 de 11

Subdirectores/as de las Direcciones Regionales

- Supervisar que el personal bajo su cargo cumpla con las disposiciones establecidas en esta política.
- Garantizar que el personal a su cargo utilice de manera adecuada los endpoints fiscales.

Unidad de Tecnologías de la Información, Subdirección de Planificación Direcciones Regionales.

- Instalar agente de antivirus en los equipos de JUNJI.
- Monitorear estado del antivirus en cada equipo de su región.
- Dar asistencia de soporte tecnológico al personal de JUNJI.
- Revisión de medios externos (pendrive y/o disco duro externo) que no contenga malware.
- Actividades que sean encomendadas por el/la Encargado/a de la Oficina de TI de DIRNAC en el ámbito de su competencia.
- Actividades que sean encomendadas por el/la Encargado/a de ciberseguridad y/o el/la Encargado de seguridad de la información de JUNJI en el ámbito de su competencia.

Funcionarios y Funcionarias de JUNJI

- Uso adecuado de Herramientas y Sistemas utilizando exclusivamente las herramientas y sistemas informáticos proporcionados por JUNJI para los endpoints de acuerdo a las indicaciones de DIRNAC siguiendo las normas y procedimientos definidos en esta política.
- Cumplimiento de la Política es de responsabilidad de cada usuario/a conocer, comprender y acatar todas las disposiciones establecidas en esta política, asegurando que sus acciones estén alineadas con los principios y normas institucionales.
- Responsabilidad en el uso de los equipos fiscales. Cada usuario/a debe hacer un uso responsable y adecuado de los medios fiscales asignados, limitándose a las actividades autorizadas y evitando cualquier acción que pueda comprometer la seguridad, integridad o buen funcionamiento de los recursos tecnológicos de JUNJI

Responsabilidades Transversales

Los endpoints de la JUNJI, incluyendo los programas, aplicaciones y archivos electrónicos, solo pueden utilizarse para fines relacionados con el desempeño de las tareas que el personal de JUNJI tenga autorizado.

Es responsabilidad de las jefaturas de cada Departamento, Unidad, Sección, Oficina, Direcciones Regionales y jardines infantiles de JUNJI, definir las tareas del personal a su cargo en la institución, que conllevan acceso a las herramientas y sistemas de la institución.

Los programas y recursos utilizados en JUNJI para conectarse a la red interna e internet deberán tener su correspondiente licencia o autorización de uso para ser utilizados. Dichos sistemas solo podrán ser instalados o desinstalados por la Sección de Tecnología de la Información (TI) de DIRNAC y por las Oficinas de TI regionales, siempre que estén aprobados por el/la Encargado/a de Ciberseguridad y la Jefatura de la Sección TI de DIRNAC.

Los funcionarios/as o usuarios/as no deben instalar programas, aplicaciones o software alguno en los equipos asignados, incluso cuando estos sean gratuitos o no requieran de permisos elevados de administrador.

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 8 de 11

La violación de las normas establecidas por la Seguridad de la Información puede conllevar la revocación de cualquier tipo de privilegio excepcional y ante la sospecha de alguna vulnerabilidad será aislado el endpoint de la red sin previo aviso.

Los funcionarios/as de la JUNJI se deberán comunicar al correo del Encargado/a de Ciberseguridad institucional para reportar eventos y posibles incidentes de seguridad de la información y Ciberseguridad.

Se prohíbe borrar información de la institución almacenada en el equipamiento computacional o aplicaciones y sistemas proporcionados por JUNJI al momento del término de la relación laboral existiendo una política de retención establecida en JUNJI.

6.3 Directrices de Configuración del Endpoint

6.3.1 Directrices de configuración

Las presentes directrices establecen los requisitos obligatorios de configuración de seguridad para todos los dispositivos finales (endpoints), tales como estaciones de trabajo, computadores portátiles y dispositivos corporativos asignados a los funcionarios y funcionarias, usuarios y usuarias y proveedores externos de la JUNJI. El propósito fundamental es mitigar las brechas de ciberseguridad, resguardar la confidencialidad de la información institucional y asegurar la alta disponibilidad de los servicios en producción.

- **Lista Blanca de Software (Whitelisting):** Los endpoints institucionales solo podrán ejecutar el software e infraestructura de ofimática explícitamente autorizados por la Sección de Tecnología de la Información y el/la Encargado/a de Ciberseguridad.
- **Restricción de Instalación Autónoma:** Queda estrictamente prohibida la instalación, descarga o ejecución de cualquier software, aplicativo o extensión que no se encuentre en el listado oficial institucional o que no cuente con la validación previa del área de ciberseguridad.
- **Uso Exclusivo Laboral:** Todo el software disponible en el endpoint debe ser utilizado exclusivamente para el cumplimiento de las funciones del cargo establecidas por la institución, prohibiéndose su uso para actividades de índole personal.

6.3.2 Restricciones sobre Software y Dispositivos No Autorizados

Se restringe la instalación, ejecución o utilización de software, aplicaciones, extensiones o servicios tecnológicos no autorizados formalmente por la Sección de Tecnología de la Información y el/la Encargado/a de Ciberseguridad.

Asimismo, no estará autorizado:

- Utilizar dispositivos personales para transferencia de información institucional.
- Conectar medios de almacenamiento no autorizados.
- Utilizar plataformas de almacenamiento en nube personales.
- Instalar software recreativo o aplicaciones no relacionadas con funciones institucionales.
- Utilizar mecanismos de compartición de internet o tethering no autorizados.
- Utilizar protocolos o herramientas de transferencia de archivos no autorizadas institucionalmente.
- Queda prohibida la conexión, instalación, sincronización o carga de teléfonos celulares y otros dispositivos móviles personales en los equipos computacionales de la organización.

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 9 de 11

6.3.3 Proceso de Solicitud de Software No Listado o Bloqueado

Cuando un funcionario/a o usuario/a requiera acceso a un software bloqueado o una nueva herramienta informática para sus funciones, deberá gestionarlo de la siguiente manera:

Debe ser autorizado y solicitado formalmente por la Jefatura de la Dirección Nacional o por el/la Director/a Regional correspondiente.

Se debe cumplimentar el "Formulario de solicitud de acceso a recursos restringidos o instalación de software", disponible en la Intranet.

La solicitud firmada debe enviarse vía correo electrónico a cbsjunji@junji.cl. El/la Encargado/a de Ciberseguridad evaluará la factibilidad técnica y los riesgos antes de otorgar o denegar el acceso.

6.3.4 Control de Dispositivos de Almacenamiento Masivo (Bloqueo de USB)

Almacenamiento Oficial en la Nube: Toda la información institucional y archivos de trabajo de la JUNJI deben almacenarse, respaldarse y compartirse única y exclusivamente a través de la nube autorizada por JUNJI. Queda prohibido el almacenamiento local definitivo en los endpoints o en nubes personales.

Dispositivos Autorizados por Excepción: Aquellos dispositivos externos que por razones de fuerza mayor sean autorizados para su uso, deberán incorporar de forma obligatoria el medio de seguridad específico que la Dirección Nacional (DIRNAC) informe oportunamente.

6.3.5 Monitoreo y Registro de Actividades

JUNJI podrá implementar mecanismos de monitoreo, registro y auditoría sobre el uso de los activos tecnológicos institucionales, incluyendo eventos de seguridad asociados a dispositivos finales, conexiones de red, transferencias de información y ejecución de software.

Dichos registros tendrán como finalidad:

- Prevenir incidentes de ciberseguridad.
- Resguardar la continuidad operacional.
- Proteger los activos institucionales.
- Investigar incidentes de seguridad.
- Cumplir obligaciones legales y regulatorias.

El acceso a los registros de monitoreo será restringido exclusivamente al personal autorizado y conforme a las funciones institucionales definidas.

6.4 Gestión, Aplicación y Cumplimiento de la Política de Ciberseguridad

6.4.1 Gestión, Evaluación y Difusión

La presente política será evaluada para modificación en JUNJI cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.

Una vez que el documento entre en vigencia el/la Encargado/a de Ciberseguridad deberá difundir en JUNJI y externos considerados en el alcance, mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrían ser página web institucional, intranet, correo electrónico al personal, capacitaciones, difusiones, entre otros canales de comunicación institucionales.

	POLÍTICA DE ENDPOINT Y CONTROL DE PERIFÉRICOS	PL-TIC-014
		Versión N.º 1
		Página 10 de 11

6.4.2 Gestión Revisión del Cumplimiento de la Política

Se revisará el cumplimiento de la presente Política en la periodicidad que lo determine el/la Encargado/a de Ciberseguridad con la finalidad de recabar información que permita definir modificaciones en pro del cumplimiento de esta.

6.4.3 Gestión Aceptación

Esta Política deberá ser aceptada por todos los/las funcionarios/as, personal a honorarios, funcionarios/as en comisión de servicio que se desempeñen en la institución, estudiantes en prácticas, pasantes y terceras partes que tengan una relación directa de acceso a la información de JUNJI que pueda afectar los activos de información. Para esto, la política será publicada y comunicada formalmente en la Intranet a través de la biblioteca de documentos procedimentales y el sitio www.junji.cl

6.4.4 Gestión Sanciones

El incumplimiento de la presente política podrá dar lugar a la aplicación de medidas administrativas, disciplinarias, contractuales, civiles o penales, conforme al Estatuto Administrativo, normativa institucional vigente y demás disposiciones legales aplicables.

Las medidas adoptadas deberán respetar el debido proceso y los procedimientos administrativos correspondientes.

6.4.5 Gestión Excepciones

Las excepciones a la presente política deberán ser debidamente justificadas, documentadas y autorizadas formalmente por el/la Encargado/a de Ciberseguridad y la jefatura correspondiente.

Toda excepción deberá considerar:

- Identificación del solicitante.
- Justificación funcional.
- Evaluación de riesgos.
- Controles compensatorios.
- Fecha de inicio.
- Fecha de expiración.
- Trazabilidad de aprobación.

Las autorizaciones excepcionales tendrán carácter temporal y deberán revisarse periódicamente.

6.4.6 Gestión Reporte de Incidentes

Todos los funcionarios y funcionarias, colaboradores o terceros comprendidos en el alcance de la presente política deberán reportar de forma inmediata cualquier incidente o sospecha de incidente de seguridad de la información o ciberseguridad que pueda afectar activos institucionales.

La gestión de incidentes será realizada conforme a los procedimientos institucionales definidos por JUNJI y la normativa vigente.

	PL-TIC-014	
	Versión N.º 1	
	Página 11 de 11	

7 ANEXOS

Al presente documento se adjuntan los siguientes Anexos:

- PL-TIC-014 -Anexo N.º1_Formulario de solicitud de acceso a recursos restringidos o Instalación de Software.
- PL-TIC-014 -Anexo N.º 2_Listado de Software autorizado en JUNJI

8 HISTÓRICO

Tabla N.º 1: *Histórico de Modificaciones*

Resumen de Modificaciones						
N.º	Versión Vigente	Versión Actualizada	Fecha (Mes/Año)	Título	Subtítulo	Descripción de la Modificación
1	1	1	S/C	S/C	S/C	Primera Versión
2						
3						