

RESOLUCIÓN EXENTA N°

MAT: APRUEBA PROCEDIMIENTO PARA LA GESTIÓN DE PERFILES DE NAVEGACIÓN Y ACCESO A INTERNET; POLÍTICA DE USO DE CORREO ELECTRÓNICO E INTERNET PARA ESTA JUNTA NACIONAL DE JARDINES INFANTILES.

SANTIAGO,

VISTOS:

1°) lo dispuesto en la Ley N° 17.301, de 1970, del Ministerio de Educación Pública, que “Crea Corporación Denominada Junta Nacional de Jardines Infantiles”; **2°)** el Decreto Supremo N° 1.574, de 1971, del Ministerio de Educación Pública, que “Aprueba Reglamento de la Ley N° 17.301, que Crea la Junta Nacional de Jardines Infantiles”; **3°)** el Decreto con Fuerza de Ley 29, de 2004, del Ministerio de Hacienda, que “Fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834 sobre “Estatuto Administrativo”; **4°)** la Ley N° 21.722, de 2024, del Ministerio de Hacienda, sobre “Presupuesto del Sector Público año 2025”; **5°)** el DFL N° 1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que “Fija Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado”; **6°)** la Ley N° 19.880, de 2003, del Ministerio Secretaría General de la Presidencia, que “Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado”; **7°)** el Decreto Supremo N° 01, de 2023, que “Nombra en el cargo de Vicepresidenta Ejecutiva de la Junta Nacional de Jardines Infantiles (JUNJI) a persona que indica y, Decreto Exento N° 61 de 2024, que establece orden de subrogancia en el cargo de Vicepresidenta Ejecutiva, ambos, del Ministerio de Educación, Subsecretaría de Educación Parvularia”; **8°)** la Resolución N° 36 de 2024, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón y demás antecedentes tenidos a la vista.

CONSIDERANDO:

1°) Que, conforme con lo previsto en el artículo 31, de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, corresponderá a los “jefes de servicio dirigir, organizar y administrar el correspondiente servicio; controlarlo y velar por el cumplimiento de sus objetivos; responder de su gestión, y desempeñar las demás funciones que la ley les asigne”.

2°) Que, a través de la Resolución Exenta N° 1022, de fecha 22 de septiembre de 2025, de la Vicepresidencia Ejecutiva de ente órgano de la Administración del Estado, se creó el Comité de Seguridad de la Información Institucional, para que, en función del marco legal y tecnológico, proponga un Sistema de Seguridad para la protección de redes, plataformas y sistemas informáticos utilizados por este Servicio.

3°) Que, la Resolución Exenta N° 1.962 de 2022, de la Contraloría General de la República, que aprueba normas de control interno, aplicables a los servicios públicos, establece en su Artículo 1, inciso primero que: *“El control interno es un proceso integral y dinámico que se adapta constantemente a los cambios que enfrenta la organización, es efectuado por la alta administración y las personas funcionarias de la entidad, está diseñado para enfrentar los riesgos y para dar una seguridad razonable del logro de la misión u objetivos de la entidad”.*

4°) Que, concordante con lo anterior, pertinente resulta aplicar con la Norma técnica NCh-ISO N° 27002, reconocida en Chile como una norma internacional de referencia para la seguridad de la información, y se utiliza para ayudar a las organizaciones a implementar



controles de seguridad efectivos, proporcionando orientación sobre como seleccionar, implementar y gestionar controles de seguridad de la información.

5º) Que, por lo indicado, el Departamento de Planificación a través de su oficina de Tecnología de la Información, elaboró un procedimiento y política de gestión en los términos señalados, los que deben ser aprobados por el respectivo acto administrativo.

RESUELVO:

I.- APRUÉBASE el “Procedimiento para la Gestión de Perfiles de Navegación y Acceso a Internet; la Política de Uso de Correo Electrónico e Internet” junto a su respectivo anexo denominado “Formulario de Solicitud Cambio de Perfil de Navegación”.

II.- ADJÚNTASE, en la plataforma de Comunicaciones Oficiales del Estado (DOCDIGITAL) el texto íntegro del “Procedimiento para la Gestión de Perfiles de Navegación y Acceso a Internet; la Política de Uso de Correo Electrónico e Internet” y su Anexo “Formulario de Solicitud Cambio de Perfil de Navegación”

III.- INCORPÓRASE al presente acto administrativo los instrumentos aprobados, pasando a formar parte integrante de la presente Resolución.

IV.- DÉJASE ESTABLECIDO que, será responsabilidad del Departamento de Planificación, a través de la Unidad u Oficina que determine, poner en conocimiento de los funcionarios de este Servicio, los instrumentos aprobados por el presente acto.

Distribución:

- Vicepresidencia Ejecutiva.
- Departamentos DIRNAC.
- Direcciones Regionales.
- Secretaría Departamento de Fiscalía y Asesoría Jurídica.
- Oficina de Partes.



Firmado por:
Daniela Paz Triviño Millar
Vicepresidenta Ejecutiva
Fecha: 03-10-2025 14:13 CLT
Junta Nacional de Jardines
Infantiles



POLÍTICA DE USO DE CORREO ELECTRÓNICO E INTERNET



JUNJI
Ministerio de
Educación

Gobierno de Chile

VERSIÓN N°1

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
	DEPARTAMENTO DE PLANIFICACIÓN SECCIÓN TECNOLOGÍAS DE LA INFORMACIÓN Versión N °1	19 páginas
GESTIÓN DE LA CIBERSEGURIDAD		

TABLA DE APROBACIÓN DOCUMENTO

Actividad	Cargo/Función	Nombre
Modificación/Elaboración	Encargado de Ciberseguridad	Diego García Rojas
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	Daniela Rubilar Balboa
Revisión Normativa	Departamento de Fiscalía y Asesoría Jurídica	Carolina Pérez Díaz
Aprobación	Vicepresidenta/e	Daniela Triviño Millar

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 1 de 19

CONTENIDOS

1	INTRODUCCIÓN	2
2	OBJETIVO	2
3	ALCANCE	3
4	NORMATIVA Y DOCUMENTOS APLICABLES	3
5	TERMINOLOGÍA	4
6	DESARROLLO POLÍTICA	5
6.1	Roles y Responsabilidades.....	5
6.1.1	Directores y Subdirectores de la Junta Nacional de Jardines Infantiles	5
6.1.2	Sección de Tecnología de la Información de DIRNAC	5
6.1.3	Encargado/a de Ciberseguridad.....	6
6.1.4	Funcionarios y Funcionarias de JUNJI.....	6
6.1.5	Oficina Mesa de Ayuda (MDA) y/u Oficina de Continuidad Operativa.....	6
6.1.6	Jefatura de la Sección Tecnología de la Información	7
6.1.7	Oficinas de Mesa De Ayuda (MDA) Direcciones Regionales	7
6.1.8	Responsabilidades Integrales	7
6.2	Uso de Internet.....	8
6.2.1	Directrices de Internet.....	8
6.2.2	Restricciones y/o Prohibiciones al Uso de internet	10
6.3	Correo Electrónico Institucional	10
6.3.1	Uso del Correo Electrónico.....	10
6.3.2	Cuentas de Correo Electrónico Genéricas	13
6.3.3	Correos Masivos.....	14
6.3.4	Listas de Distribución o Grupos de Correo.....	14
6.3.5	Restricciones al Uso y Contenido del Correo Electrónico.....	15
6.3.6	Gestión de Correo Electrónico por Término de Relación Laboral.....	16
6.4	Redes sociales institucionales	16
6.4.1	Protocolo de Uso de Redes Sociales Institucionales	16
6.5	Recursos Restringidos de Internet.....	17
6.5.1	Instructivo para Solicitar Acceso a Recursos Restringidos de Internet.....	17

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 2 de 19

6.6	Gestión, Aplicación y Cumplimiento de la Política de Ciberseguridad	17
6.6.1	Evaluación y Difusión	17
6.6.2	Revisión del Cumplimiento de la Política	18
6.6.3	Aceptación	18
6.6.4	Sanciones	18
6.6.5	Excepciones	18
7	ANEXOS	18
8	HISTORICO	19

1 INTRODUCCIÓN

Para asegurar el óptimo desempeño de los sistemas tecnológicos, así como de los servicios vinculados a Internet y la mensajería electrónica, la Junta Nacional de Jardines Infantiles, en adelante denominada JUNJI, ha implementado una serie de normas y pautas de uso aceptable para los equipos y servicios de JUNJI. Estas disposiciones buscan garantizar que los recursos entregados por JUNJI sean empleados de manera adecuada, protegiendo tanto al personal JUNJI como a la institución frente a posibles riesgos que puedan afectar la integridad de los sistemas y la información que estos contienen.

2 OBJETIVO

Facilitar la comunicación efectiva y segura tanto de usuarios internos como externos, la cual debe ser rápida y eficiente entre funcionarios, departamentos, unidades, secciones, oficinas, jardines infantiles y proveedores de la institución para la continuidad de los distintos procesos en los cuales es necesaria esta comunicación, servicio o acceso a sistemas de información tanto internos como externos asegurando la confidencialidad, integridad y la disponibilidad de la información.

Objetivos específicos

- ✓ Definir y regular el uso de los sistemas de información y el servicio de mensajería (correo institucional), estableciendo criterios para accesos o restricciones de navegación en sitios web, servicios de conexión a Internet y uso del servicio de mensajería en la institución.
- ✓ Reducir riesgos que puedan afectar las operaciones y normar el manejo, la protección y resguardo de la información asegurando la confidencialidad.
- ✓ Definir categorías generales y específicas para gestionar el acceso o bloqueo de diversos sitios web, y asegurar la continuidad de los servicios de correo electrónico institucional.
- ✓ Minimizar posibles interrupciones o suspensión de los servicios

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 3 de 19

- ✓ Proporcionar a los usuarios/as una orientación clara sobre los requisitos mínimos que deberán cumplirse en relación con el uso del correo electrónico institucional proporcionado por la entidad, así como las consecuencias derivadas de un uso inapropiado.
- ✓ Prevenir mediante monitoreos y configuraciones la aparición de latencia o lentitud, interrupciones en los servicios de comunicación institucional que puedan generar demoras o afectar la velocidad y calidad del servicio.
- ✓ Promover entre los usuarios y usuarias una cultura de responsabilidad en el manejo de los sistemas y la mensajería electrónica, con el fin de prevenir situaciones que expongan a riesgos, amenazas, vulnerabilidades o fallas en los sistemas informáticos, servicios de red y datos institucionales, lo que podría resultar en sanciones impuestas por la Agencia Nacional de Ciberseguridad y/o Agencia de Protección de los Datos Personales.
- ✓ Establecer las medidas requeridas para resguardar la privacidad de la información, fomentando una utilización apropiada de los sistemas tecnológicos y los servicios vinculados a Internet.

3 ALCANCE

Esta política y las asociadas a esta son de cumplimiento obligatorio para todos los funcionarios de planta, a contrata, honorarios y estudiantes en práctica que cumplan funciones tanto en oficinas como a todo personal externo que presten servicios profesionales y utilicen los servicios de red, sistemas o mensajería institucionales y que tengan 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°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. 17.336 de 1970. [Ministerio de Educación Pública]. Sobre Propiedad Intelectual. Fecha de vigencia a contar del 02 de octubre de 1970.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 4 de 19

Ley Nro. 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 y con fecha diferida de vigencia a contar 01 de diciembre 2026.

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

Ley Nro. 21.180, de 2019, Sobre Digitalización del Estado, del Ministerio Secretaría General de la Presidencia.

Resolución Exenta N° 757 de 2019 [Junta Nacional de Jardines Infantiles]. Aprueba Política General de Seguridad de la Información, Octava Versión, Fecha de vigencia a contar 21 de noviembre 2019.

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.

Normativa Interna [Junta Nacional de Jardines Infantiles]. Política control de acceso lógico de la Junta Nacional de Jardines Infantiles. 2021.

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.

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 USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 5 de 19

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, usuarios, proveedores y audiencias institucionales.

6 DESARROLLO POLÍTICA

6.1 Roles y Responsabilidades

6.1.1 *Directores y Subdirectores de la Junta Nacional de Jardines Infantiles*

- Supervisar que el personal bajo su cargo cumpla con las disposiciones establecidas en esta política.
- Autorizar las solicitudes de acceso a recursos de internet que se encuentren bloqueados, mediante los formularios correspondientes.
- Gestionar la creación de cuentas genéricas para las Direcciones Regionales a su cargo con un responsable de su administración.
- Informar a la Sección de Tecnología de la Información sobre las altas y bajas del personal dentro de su área de responsabilidad.
- Garantizar que el personal a su cargo utilice de manera adecuada las contraseñas y evite compartirlas.
- Solicitar la creación de cuentas genéricas de correo electrónico y designar al responsable de su administración y uso.

6.1.2 *Sección de Tecnología de la Información de DIRNAC*

- Diseñar y gestionar los sistemas informáticos destinados al uso de internet y la mensajería electrónica dentro de la institución.
- Coordinar la creación y desactivación de cuentas institucionales para el acceso a recursos de navegación y correo electrónico.
- Servir como punto de contacto para brindar orientación, asesoría, actualizaciones y solución de problemas relacionados con los sistemas informáticos.
- Proponer y ejecutar configuraciones de seguridad en los sistemas informáticos y servicios asociados a internet.
- Instalar y mantener las aplicaciones 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 los perfiles de navegación en la red institucional.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 6 de 19

- Aislar la red de visitas de los recursos internos de JUNJI para proteger la integridad y seguridad de la información institucional.

6.1.3 Encargado/a de Ciberseguridad

- 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 internet.
- Garantizar la correcta aplicación de la política y brindar apoyo a las oficinas técnicas responsables de la administración y gestión del uso de internet y sistemas informáticos conectados a la red.
- 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 sitios web o servicios en línea 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.
- 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.
- Gestionar y controlar los perfiles de navegación en la red institucional.
- Evaluar y autorizar o rechazar solicitudes de acceso a recursos de internet, 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.
- Revisar en conjunto con Mesa de Ayuda (MDA) los dominios de correo electrónico que deban ser bloqueados por razones de seguridad.
- Actualizar periódicamente la presente política, con el objetivo de asegurar su idoneidad, eficiencia y efectividad continua en el tiempo.

6.1.4 Funcionarios y Funcionarias de JUNJI

- Uso adecuado de Herramientas y Sistemas utilizando exclusivamente las herramientas y sistemas informáticos proporcionados por JUNJI para navegar en internet y enviar mensajería instantánea, siguiendo las normas y procedimientos definidos en esta política.
- Cumplimiento de la Política es de responsabilidad de cada usuario/a conocer, entender 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 Internet y Correo Electrónico de cada usuario/a, deberá hacer un uso responsable y adecuado del acceso a internet y del correo electrónico institucional, limitándose a las actividades autorizadas y evitando cualquier acción que pueda comprometer la seguridad, integridad o buen funcionamiento de los recursos tecnológicos de JUNJI.

6.1.5 Oficina Mesa de Ayuda (MDA) y/u Oficina de Continuidad Operativa

- Eliminar correos entrantes de forma masiva que signifiquen un riesgo o que vayan en contra de esta política.
- Bloquear dominios que representen una amenaza de seguridad.
- Revisar y ejecutar permisos de configuración general de cuentas de correos de la institución.
- Deshabilitar toda cuenta de correo electrónico genérica que no cuente con un responsable definido.
- Crear, inventariar y administrar listas o grupos de correos oficiales de JUNJI.
- Actividades que sean encomendadas por el Encargado de la Sección de TI.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 7 de 19

6.1.6 Jefatura de la Sección Tecnología de la Información

- Aprobar en conjunto al Encargado/a de Ciberseguridad las aplicaciones o software que puedan ser instalados en la institución.
- Evaluar y ejecutar modificaciones de parámetros de configuración general de las cuentas de correo electrónico.

6.1.7 Oficinas de Mesa De Ayuda (MDA) Direcciones Regionales

- Configurar o asesorar para la configuración del Multifactor de autenticación de Microsoft para el personal de JUNJI.
- Dar asistencia de soporte tecnológico al personal de JUNJI.
- Actividades que sean encomendadas por el/la Encargado/a de la Oficina de TI en el ámbito de su competencia.

6.1.8 Responsabilidades Integrales

Los sistemas de la información de JUNJI, incluyendo los programas, aplicaciones y archivos electrónicos, sólo 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 conlleven 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 aprobadas 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.

La violación de las normas establecidas por la Seguridad de la Información puede conllevar la revocación de cualquier tipo de privilegio de uso de los sistemas, sitios y Servicios de Información de JUNJI.

Los funcionarios/as de 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.

Los funcionarios/as de JUNJI son responsables de gestionar la seguridad de su propia información como de sus cuentas (usuarios y contraseñas). El uso de contraseñas debe ser de acuerdo con la "Política Uso de Contraseñas". Cada jefatura deberá velar que el personal que tiene a su cargo realice un buen uso de estas y no las comparta por ningún motivo.

Las cuentas (usuarios y contraseñas) son asignadas de forma individual y no pueden ser compartidas con terceros. Los/las funcionarios/as o usuarios/as de JUNJI son responsables también por el tráfico y el contenido de la información de las cuentas asignadas. El mal uso de una cuenta institucional puede conllevar la revocación de cualquier tipo de privilegio de uso, de acuerdo con las normas establecidas por JUNJI declaradas en la presente política.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 8 de 19

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

6.2 Uso de Internet

6.2.1 Directrices de Internet

Los sistemas de comunicación y acceso a internet de JUNJI deben ser utilizados exclusivamente como una herramienta de trabajo conforme a las funciones de cargo establecidas por la institución y no para actividades personales. Por lo tanto, cualquier sitio no relacionado a fines laborales podrá ser bloqueado en beneficio de la institución, tales como: radios, revistas, streaming, tiendas de compra, entre otros. Esto será revisado por la Sección de Tecnología de la Información y el/la Encargado/a de Ciberseguridad de forma periódica.

La Sección de Tecnología de la Información en conjunto el/la Encargado/a de Ciberseguridad de la JUNJI, realizarán bloqueos de sitios que representen amenazas de seguridad, integridad o disponibilidad de los recursos internos o activos de información a través de herramientas tecnológicas que permita esto.

La Sección de Tecnología de la Información, en colaboración con el/la Encargado/a de Ciberseguridad de JUNJI, implementará medidas de Seguridad en la Red para mitigar posibles brechas de Ciberseguridad. Además, deberán proteger los recursos de la red institucional para prevenir la indisponibilidad de servicios. Para lograr esto, podrán llevar a cabo acciones destinadas a asegurar la calidad y estabilidad de los Servicios de Red, realizando bloqueos o limitando el tráfico de red con el/la profesional de redes de JUNJI.

El acceso a la red se encuentra disponible para todos los funcionarios/as o usuarios/as de JUNJI, sin embargo, existen diferentes tipos de perfiles de navegación limitados por la necesidad de acceso que se requiera según funciones del cargo y/o según sea autorizado por las jefaturas de la Dirección Nacional o el/la Director/a Regional correspondientemente, además del Encargado/a de Ciberseguridad. El proceso de solicitud de modificación de perfil de navegación se encuentra descrito en el "Procedimiento de Cuentas Privilegiadas, accesos restringidos y VPN" vigente, donde se indica que se deberá realizar la solicitud a cbs@junji.cl y adjuntar el formulario correspondiente ubicado en la Intranet.

La Sección de Tecnología de la Información en conjunto con el/la Encargado/a de Ciberseguridad de la JUNJI crearán y modificarán perfiles de navegación diferenciados según las funciones de cargo de los funcionarios/as o usuarios/as de JUNJI.

Los funcionarios/as de JUNJI son responsables del buen uso de su navegación de internet y buen uso de recursos de red disponible. Por lo tanto, el acceso a la red proporcionada por JUNJI solo debe utilizarse para fines laborales acorde a las funciones del cargo y no para fines personales, como, por ejemplo: escuchar música en YouTube u otro servicio de audio y video, ya que afecta a los recursos de red proporcionados por JUNJI y a su vez afecta la calidad de los servicios utilizados para fines laborales como los sistemas de información en producción y utilizados para los distintos procesos institucionales y de los aplicativos de ofimática o software utilizados por unidades específicas para realizar sus funciones.

Al trabajar de forma remota solo se podrá utilizar las herramientas de VPN provistas por la Sección de Tecnología de la Información y su uso e instalación es solo institucional asignados a los usuarios. Los proveedores externos deberán realizar su propia instalación de acuerdo con las características establecidas por la institución.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 9 de 19

Las operaciones realizadas a través de internet por el personal de JUNJI podrán ser intervenidas y auditadas por la Sección de Tecnología e Información o el/la Encargado de Ciberseguridad con el fin de prevenir o actuar en función de la calidad de servicios, eventos o incidente de ciberseguridad.

Las soluciones inalámbricas para visitas deben contar con un portal cautivo para que los invitados o personas externas a JUNJI que necesiten conexión a internet sólo puedan acceder de forma controlada. Además, esta red de visitas debe estar configurada en un segmento de red aislado, sin acceso a los recursos institucionales internos. Esto será verificado por el/la Encargado/a de Ciberseguridad.

Toda información de red entrante y saliente a internet es monitoreada y registrada por la Sección de Tecnología de la Información con el propósito de garantizar el nivel de servicio de navegación a internet, priorizando las comunicaciones que la institución requiere mantener con otras entidades gubernamentales y/o privadas, necesarias para el funcionamiento de los sistemas informáticos institucionales.

Solo podrá acceder a los perfiles o cuentas oficiales de redes sociales de JUNJI, los funcionarios/as o usuarios/as pertenecientes al Departamento de Comunicaciones de la Dirección Nacional y Regionales y según sus funciones designadas. Respecto al uso de redes sociales revisar "Anexo 14.1: Protocolo de uso de redes sociales" de JUNJI.

Cuando los funcionarios/as o usuarios/as de JUNJI requieran el acceso a un sitio que se encuentre bloqueado, debe ser autorizado y solicitado por la Jefatura de Dirección Nacional o por el/la Subdirectora/o Regional en caso de que corresponda mediante el Formulario solicitud de acceso a recursos restringidos de internet o Formulario de acceso a páginas bloqueadas publicado en la Intranet y debe ser enviado al email cbs@junji.cl. Este será evaluado por el/la Encargado/a Ciberseguridad para ver factibilidad de otorgar el acceso.

Aquellos sitios de internet que se encuentren bloqueados pero que estén relacionados a actividades generales de JUNJI, podrán ser liberados siempre que el sitio no presente problemas de seguridad al utilizarlo. Para lo anterior, se deberá enviar una solicitud por la jefatura directa para liberar el sitio a cbs@junji.cl sin la necesidad de adjuntar un formulario de acceso y deberá ser revisada y aprobada por el/la Encargado/a de Ciberseguridad. Algunos ejemplos son: sitios de establecimientos educacionales, municipios, entre otros.

Los funcionarios/as o usuarios/as de JUNJI que se encuentren a cargo de promocionar eventos comunicacionales de JUNJI o de otra entidad pública que sea transmitido a través de YouTube u otra plataforma que se encuentre bloqueada, deberá completar el formulario correspondiente publicado en la Intranet, que deberá ser firmado por la jefatura directa del solicitante y enviado a cbs@junji.cl como mínimo con 48 horas de anticipación al evento en cuestión.

Los navegadores de internet que podrán ser usados por el personal de JUNJI serán definidos por la sección de Tecnología e Información y el/la Encargado/a de Ciberseguridad. Siendo los navegadores por defecto Microsoft Edge, Google Chrome y excepcionalmente Safari, dependiendo del sistema operativo del equipamiento.

El/la funcionario/a responsable de organizar o gestionar capacitaciones o cursos internos de los cuales los sitios o plataformas que se deban utilizar se encuentren bloqueadas, deberán realizar una solicitud para que a los y las participantes de dichos cursos puedan contar con un perfil de navegación a internet especial para capacitaciones. Esta solicitud, se debe realizar al menos con 48 horas de anticipación al correo cbs@junji.cl adjuntando el formulario correspondiente ubicado en la Sección de Seguridad de la Información en la Intranet Institucional. A su vez, deberán trabajar de forma colaborativa con la Sección de Tecnología de la Información, con el fin de ir adecuando o modificando el listado de accesos a sitios o plataformas que se deben habilitar en función de las capacitaciones o cursos a realizar.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 10 de 19

6.2.2 Restricciones y/o Prohibiciones al Uso de internet

- a) Se prohíbe descargar desde internet contenido, archivos ejecutables que se encuentren en sitios cuestionables, desconocidos o inseguros que representen una amenaza de seguridad, esto se realizará con el apoyo de las herramientas tecnológicas necesarias y realizando auditorías periódicas.
- b) Se prohíbe almacenar información institucional en sitios o nubes de almacenamiento virtual provisto por terceros como Dropbox, Google Drive, WeTransfer, entre otros. Solo se debe utilizar para este propósito la nube oficial de almacenamiento de JUNJI. Esta es **OneDrive de Microsoft 365 de JUNJI**.
- c) Se prohíbe el uso de herramientas en línea no provistos o autorizados por la Sección de Tecnología de la Información y el/la Encargado/a de Ciberseguridad para trabajar documentos o información de JUNJI. Entre ellos, editores de documentos de textos, de planillas, de imágenes, de PDF, entre otros. Lo anterior, es para evitar posibles filtraciones de información de la institución en Internet.
- d) No está permitido utilizar los equipos computacionales entregados por JUNJI para actividades no relacionadas con las asignadas a su función. El cumplimiento de estas restricciones se regulará de acuerdo con el perfil del personal. En particular está prohibido lo siguiente:
- Descargar e instalar aplicaciones de audio/video vía internet de radios online y de aplicaciones como: Spotify, Netflix, entre otros medios de streaming no relacionados a la función del cargo.
 - Cargar y/o descargar archivos de música no relacionados con la función del cargo.
 - Cargar y/o descargar archivos de imágenes y videos no relacionados con la función del cargo.
 - Cargar y/o descargar juegos o jugar online.
 - Instalar sistemas de telecomunicaciones ajenos a los corporativos.
 - Construcción y/o hosting de sitios web personales o ajenos a la institución.
 - Utilizar el Protocolo de Transferencia de Ficheros FTP.
 - Transferencia de datos a través de Protocolo de Transferencia Segura de Archivos u otros no autorizados bajo convenios de interoperabilidad o de colaboración con entidades externas o de estado.

6.3 Correo Electrónico Institucional

6.3.1 Uso del Correo Electrónico

- a) El Departamento de Gestión de las Personas por medio de su Sección y oficina de Personal serán los responsables de notificar a la Sección de Tecnología de la Información, a través de la casilla de mda@junji.cl cuando se deba habilitar o deshabilitar una cuenta de correo electrónico para un nuevo ingreso o egreso de funcionarios/as (usuarios/as) de JUNJI.
- b) Una cuenta de correo electrónico consta de dos partes: el nombre de usuario al costado izquierdo y el dominio al costado derecho, ambos unidos por el símbolo @. El nombre de usuario está formado por el primer nombre, un punto y el primer apellido seguido de un "@junji.cl" o "junjired.cl, resultando finalmente con el siguiente **formato: "nombre.apellido@junji.cl" o "nombre.apellido@junjired.cl".**

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 11 de 19

c) Si la cuenta de correo electrónico que se requiere utilizar no estuviese disponible, el administrador de correo institucional podrá modificar el formato establecido, eligiendo modificar prioritariamente la sección del apellido, en la cual se puede ir añadiendo las letras iniciales del segundo apellido hasta que la cuenta de correo electrónico esté disponible para su uso. El personal de MDA dependiendo del caso, podría usar otro criterio alternativo.

d) Las cuentas de correo electrónicas institucionales podrán por defecto enviar y recibir contenido de hasta un tamaño de "20 MB". Si el adjunto tuviese un tamaño mayor, este no se podrá enviar ni recibir. La modificación de este tamaño se realizará tras una evaluación técnica llevada a cabo por el/la Encargado/a de Ciberseguridad, junto con la Jefatura de la Sección de TI, de acuerdo con los roles y funciones definidos por el Servicio. En casos excepcionales, se podrá solicitar un aumento de espacio de este recurso. Para ello, la jefatura de unidad, oficina o jefatura superior jerárquica deberá enviar un correo electrónico con esta solicitud a mda@junji.cl donde posteriormente, una vez analizada la particularidad del requerimiento, podrá ser autorizado o rechazado por el/la Encargado/a de Ciberseguridad.

e) Toda cuenta de correo electrónico institucional está directamente vinculada al personal de la JUNJI, el cual es responsable del contenido y de los archivos adjuntos en cada mensaje.

f) Los funcionarios/as o usuarios/as de JUNJI con una cuenta de correo electrónico institucional asignada, son responsables de gestionar la mantención, administración y limpieza en su cuenta, dejando la bandeja de entrada libre de spam, publicidad, correos personales, entre otros. Además, debe priorizar la gestión de los correos más recientes y relevantes. Es importante considerar que cada cuenta de correo electrónico individual dispone de un límite máximo de almacenamiento de 100 GB.

g) El resguardo de las claves de acceso (contraseña) al correo electrónico (o cuentas de acceso) es de exclusiva responsabilidad de los funcionarios/as o usuarios/as de JUNJI. Estas no se deberán divulgar, compartir ni anotar en lugares visibles o de fácil acceso para terceros.

h) Los funcionarios/as o usuarios/as de JUNJI deberán utilizar un lenguaje respetuoso en sus mensajes con terceros, internos o externos y estos de ninguna forma podrán contener contenido difamatorio, insultante, injurioso, amenazador, ofensivo, obsceno, racista, sexista o violencia de género.

i) Los funcionarios/as o usuarios/as de JUNJI deben utilizar el correo electrónico institucional solo para fines laborales.

j) Como regla general, toda información de JUNJI no deberá ser compartida con personas externas al Servicio sin la debida autorización escrita de la respectiva jefatura y/o el/la Encargado/a de Ciberseguridad. Siempre se deberá tener en cuenta que existe un riesgo de interceptación de la información, por esta razón se recomienda no enunciar el contenido de información confidencial o sensible en el título o asunto de un correo electrónico.

k) Todo correo electrónico que **conservar información sensible o confidencial deberá poseer una etiqueta de seguridad confidencial**, en la que solo el destinatario de correo pueda visualizar el contenido.

l) Los funcionarios/as o usuarios/as de JUNJI que presenten interrogantes sobre la seguridad de la información que necesita enviar por correo electrónico, debe consultar primero con su jefatura. En caso

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 12 de 19

de que la jefatura también tenga dudas al respecto, se debe consultar a él/la Encargado/a de Ciberseguridad.

m) Los funcionarios/as o usuarios/as de JUNJI deberán contar con una firma de correo electrónico que actúe como identificador. Esta firma deberá contener al menos los siguientes puntos: nombre, apellido, cargo, Departamento, unidad, sección, oficina, Dirección Regional, Subdirección y jardines infantiles con el fin de que el receptor del mensaje identifique con certeza la identidad del remitente y su procedencia.

n) Para la utilización del correo electrónico institucional sólo se podrá acceder mediante el gestor de correo de Outlook de la suite de Office perteneciente a Microsoft 365. Para lo anterior, se puede utilizar de forma local con la aplicación instalada, ya sea en un equipo computación o dispositivo móvil o desde la página web oficial de Microsoft 365.

o) En relación con el punto anterior, es obligatorio utilizar un Multifactor de Autenticación o MFA de Microsoft para acceder a las cuentas de correo institucional. Esta tecnología permite tener un segundo método de verificación para el acceso y de esta manera agregar una capa adicional de seguridad de ciberseguridad. Los funcionarios/as o usuarios/as de JUNJI que cuente con celulares institucionales deben utilizar obligatoriamente el MFA desde estos dispositivos. La configuración del MFA será realizada por el personal de MDA en Dirección Nacional o las Oficinas de TI a nivel nacional según corresponda.

p) Los funcionarios/as o **usuarios/as de JUNJI que se ausenten** de sus labores debido al uso de feriados legales, licencias médicas, permisos administrativos u otros, deberán configurar una respuesta automática de correo electrónico, donde comunique que se encontrará ausente por un período de tiempo, especificando el rango de fechas de ausencia e indicando el nombre y correo electrónico de quien será el reemplazante por dicho periodo.

q) Para los archivos que no se puedan compartir por correo electrónico debido a su tamaño, se deberá utilizar la herramienta OneDrive o SharePoint, la cual corresponde a la nube de almacenamiento oficial de JUNJI. Excepcionalmente se podrá utilizar otro medio de transferencia por única vez solo si es autorizado por el/la Encargado/a de Ciberseguridad.

r) Siempre que se utilice OneDrive o SharePoint se debe compartir solo a los usuarios específicos que se requiera que accedan a la carpeta o archivo compartido. Solo excepcionalmente se debe compartir en la modalidad de **"cualquier usuario"** cuando se requiera dejar un vínculo público por temáticas específicas.

s) Se podrá compartir información reservada a través de OneDrive o SharePoint con terceros solo por medio de un convenio de colaboración o por razones de buen servicio en base a las atribuciones o facultades otorgadas por la constitución o legales.

t) El correo y las aplicaciones de Microsoft 365 no se podrán utilizar desde fuera de Chile, con el fin de prevenir ciberataques desde el extranjero. Si el personal del Servicio requiere acceder desde otro país, la jefatura de dicha persona deberá realizar una solicitud mediante un correo a cbs@junji.cl, identificándose como la jefatura del solicitante e incluyendo el nombre del solicitante, el correo del solicitante, el país desde el cual accederá, el período de tiempo y finalmente la debida justificación. Esta solicitud será aprobada o rechazada por el/la Encargado/a de Ciberseguridad. Además, si no se envía la información indicada previamente, la solicitud será rechazada de forma automática.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 13 de 19

u) La Sección de TI podrá eliminar correos de forma masiva que sean identificados como maliciosos, publicidad, spam, temáticas no laborales que generen incertidumbre, ofensas, no autorizados y que en general infrinjan la presente Política. Esto deberá ser revisado en conjunto con el/la Encargado/a de Ciberseguridad.

v) La Sección de TI podrá bloquear dominios que se encuentren en lista negra, sean inseguros o representen una amenaza de seguridad para la JUNJI. Esto deberá ser revisado en conjunto con el/la Encargado/a de Ciberseguridad.

6.3.2 Cuentas de Correo Electrónico Genéricas

a) La creación de cuentas genéricas, las cuales son destinadas a representar un servicio de envío y/o recepción de mensajería electrónica colectiva, se gestionarán a través de la jefatura de cada Departamento, Sección u otro cargo de jefatura o representante, quien deberá solicitar vía correo electrónico a mda@junji.cl indicando el nombre tentativo de la dirección de correo electrónico y quien será el responsable de la cuenta. El/la responsable de la cuenta será a quien se configure el Multifactor de autenticación (MFA) obligatorio por cada cuenta existente. La solicitud de creación de una cuenta de correo genérica deberá realizar al menos con un día hábil de anterioridad. La factibilidad de creación de una cuenta genérica estará bajo la condición de que exista el licenciamiento adecuado.

b) Las cuentas de correo electrónico genéricas tendrán un espacio de almacenamiento **total de 50 GB**.

c) Toda cuenta correo genérica debe contar con un responsable identificado. Este deberá aparecer en la descripción de dicha cuenta.

d) La MDA podrá deshabilitar toda cuenta de correo genérica que no cuente con un responsable.

e) El personal a cargo de la cuenta de correo genérica es quien debe resguardar su correcto uso, ya que todo el contenido que se transmita desde dicha cuenta es de su responsabilidad. Este también será el responsable de asegurar que la cuenta tenga una firma de correo configurada. De no saber configurar la firma, debe solicitar asistencia a mda@junji.cl.

f) La firma de correo electrónico de una cuenta genérica debe contener el nombre del usuario/as Departamento, Sección u oficina a la que pertenezca y debe contener la Dirección Regional o Nacional a la que pertenece. Esto, utilizando el formato para firmas de correo.

g) La firma de correo electrónico de una cuenta genérica podrá no incluirse al enviar un mensaje de correo, siempre que este mensaje contenga un comunicado donde se logre identificar la procedencia de la cuenta.

h) Las cuentas de correo genérica deben contar obligatoriamente con un Multifactor de autenticación o MFA. El/la responsable de la cuenta debe administrar el MFA asociado a dicha cuenta.

i) Las cuentas genéricas no reemplazan en ningún momento las cuentas únicas e identificables de los funcionarios/as o usuarios/as de JUNJI. Estas serán utilizadas para fines y temáticas específicas, siendo una de sus principales funciones el envío de correo masivo a través de listas de distribución o grupos de correos oficiales.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 14 de 19

6.3.3 Correos Masivos

A continuación, se indican las directrices a seguir para la gestión de correos masivos:

- a) Se podrán realizar envíos de correos masivos desde cuentas institucionales genéricas que se encuentren autorizadas y mediante listas de distribución o grupos de seguridad oficiales creados por la MDA y en casos excepcionales se podrán enviar a destinatarios individuales sin grupos de correo asociados según la temática de uso de la cuenta de correo genérica.
- b) Cada Jefatura, encargados/as, representantes de equipos de trabajo, podrán enviar correos electrónicos consideramos como masivos desde sus cuentas individuales con fines laborales, solo a través de listas de distribuciones oficiales propias de sus respectivos equipos o a las que hayan sido autorizados por MDA.
- c) Si se requieren enviar correos masivos desde una cuenta genérica a la lista de distribución o grupo de correo que abarca a todo el personal de JUNJI o de las diferentes direcciones regionales, la jefatura de donde pertenece la cuenta genérica debe solicitar autorización a la Jefatura de Gabinete o quien esta designe, por medio de un correo electrónico. Una vez que sea aprobado por escrito, la jefatura solicitante deberá reenviar el correo a mda@junji.cl con la autorización correspondiente y realizar la solicitud para que se configuren los permisos adecuados para el envío de correo masivo a dicho grupo de correo.
- d) En relación con las Asociaciones Gremiales, si requieren enviar correos masivos desde una cuenta genérica a la lista de distribución o grupo de correo que abarca a todo el personal de JUNJI o de las diferentes Direcciones Regionales, deberá ser gestionado y autorizado por la Unidad Asesora Gremial. Una vez que sea aprobado por escrito, la jefatura solicitante deberá reenviar el correo a mda@junji.cl con la autorización correspondiente y realizar la solicitud para que se configuren los permisos adecuados para el envío de correo masivo a dicho grupo de correo.
- e) Se prohíbe el envío de correos masivos de ofertas de compras o ventas, así como también cualquier tipo de cartas, notas en cadena, publicidad, opiniones o correos que pudiesen afectar la imagen de los funcionarios/as de JUNJI.
- f) Se prohíbe el envío de mensajes masivos que comprometan el prestigio o nombre de JUNJI o de alguno de sus miembros.
- g) Se prohíbe falsificar encabezados de correos electrónicos, es decir utilizar nombres de dominio que sean inválidos o inexistentes u otras formas engañosas de enviar correo electrónico.

6.3.4 Listas de Distribución o Grupos de Correo

Las listas de distribución o grupos de seguridad, como su nombre lo indica, son grupos con dos o más destinatarios de correos de funcionarios/as o usuarios/as de JUNJI. A continuación, se indican sus directrices:

- a) Los funcionarios/as o usuarios/as de JUNJI podrán utilizar las listas de distribución o grupos de seguridad oficiales autorizados que hayan sido creados por la MDA.
- b) Estos grupos de seguridad o de distribución corresponderán y se crearán de acuerdo con la estructura orgánica vigente y según la resolución exenta que describa dicha estructura.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 15 de 19

c) En forma paulatina y planificada se procederá a eliminar listas de distribución que no se ajusten a la estructura orgánica vigente.

6.3.5 Restricciones al Uso y Contenido del Correo Electrónico

a) Los funcionarios/as o usuarios/as de JUNJI tienen prohibido acceder a la cuenta de correo de otro usuario y tomar su identidad.

b) Está prohibido personificar a otra persona en un correo electrónico mediante el uso de encabezados falsificados u otra información personal. Esto incluye tomar el nombre de usuario/a de otra persona y hacerse pasar por ella al enviar correos electrónicos.

c) Los funcionarios/as o usuarios/as de JUNJI deben respetar la naturaleza confidencial de los datos que puedan ser de su conocimiento por el cargo de su función y no compartirlos con terceros no autorizados.

d) Se prohíbe utilizar cuentas individuales de correo electrónico para enviar correos de forma masiva a excepción de lo indicado en el **Ítem "8.3 Correos Masivos"**

e) Se prohíbe el uso de seudónimos u otras formas para ocultar su identidad. En todos los mensajes debe estar claramente identificado el origen y propietario del mensaje.

f) Se prohíbe el envío de publicidad o cualquier información de tipo comercial por correo institucional.

g) Los mensajes contenidos en el correo institucional no podrán ser contrarios a las disposiciones del orden público y al respeto de los derechos fundamentales de las personas.

h) No se debe enviar por correo institucional, contenidos que no tengan relación con el trabajo, tales como: videos, imágenes, archivos de audio, etc., a fin de no sobrecargar la red institucional.

i) Se prohíbe utilizar la cuenta de correo electrónico institucional para emitir opiniones en espacios de discusión interna o externa a la institución, listas temáticas u otras instancias de naturaleza polémica, que pueda crear conflictos al interior de la institución.

j) Se prohíbe descargar o ejecutar archivos adjuntos de remitentes desconocidos. Ante cualquier duda de la confiabilidad de algún adjunto, deberá preguntar a Encargado/a de Ciberseguridad.

k) Los funcionarios/as o usuarios/as de JUNJI deberán protegerse contra archivos adjuntos sospechosos que provengan de remitentes conocidos que pudieron verse afectados por algún tipo de ataque cibernético. En estos casos no se debe abrir el adjunto y se debe solicitar asistencia a mda@junji.cl.

l) Se prohíbe difundir cualquier listado de contactos, ya sea de correos electrónicos o contactos telefónicos por cualquier medio electrónico o impreso para propósitos que no sean de uso institucional.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 16 de 19

- m) Se prohíbe el uso de correos electrónicos personales con fines laborales; se deberán emplear exclusivamente las herramientas proporcionadas y autorizadas por JUNJI para la comunicación electrónica.
- n) Los funcionarios/as o usuarios/as de JUNJI no podrán sincronizar su correo institucional o el de cuentas de correo genéricas en sistemas, servicios, páginas web externas u otros que no estén previamente autorizados por el/la Encargado/a de Seguridad de Ciberseguridad.
- o) El correo electrónico institucional no debe utilizarse para suscribirse a boletines, ofertas comerciales, servicios o sitios web que no estén relacionados con las funciones laborales institucionales.
- p) Se prohíbe el uso de aplicaciones de terceros no autorizadas para la gestión de correos electrónicos institucionales (softwares, combinar correspondencia, entre otros).
- q) Se prohíbe redireccionar automáticamente los correos electrónicos institucionales a cuentas externas sin autorización previa de Encargado/a de Seguridad de Ciberseguridad.
- r) Se prohíbe utilizar imágenes de perfiles de cuentas institucionales que sean inapropiadas en contexto laboral, donde se presenten imágenes: ofensivas, sexualizadas, ideológicas, publicitarias o de propaganda.
- s) Se prohíbe eliminar o borrar correos electrónicos de las cuentas institucionales producto del término de relación laboral con JUNJI.

6.3.6 Gestión de Correo Electrónico por Término de Relación Laboral

- a) El Departamento de Gestión de las Personas, informará diariamente mediante correo electrónico institucional a la Sección de Tecnologías de la Información a la casilla mda@junji.cl cuando un/a funcionario/a sea desvinculado por las distintas causales. Se procederá a respaldar y deshabilitar dicha cuenta de correo electrónico institucional.
- b) Las cuentas de correos institucionales una vez deshabilitadas contarán con un respaldo de máximo de 2 años atrás al momento de deshabilitar la cuenta. Estos quedarán disponibles por 2 años desde el momento de haber deshabilitado la cuenta. Al transcurrir los 2 años, los respaldos serán eliminados. Podrían generarse excepciones, siempre y cuando se cuente con los recursos y licenciamiento necesario para realizarlo.

6.4 Redes sociales institucionales

6.4.1 Protocolo de Uso de Redes Sociales Institucionales

El siguiente protocolo está compuesto por las reglas y conductas que deberán seguir los funcionarios o usuarios de JUNJI autorizado para acceder a redes sociales oficiales de JUNJI. Este documento incluye las redes sociales de Facebook, LinkedIn, YouTube, X, Instagram, entre otros. Las directrices son las siguientes y no está permitido:

- a) Usar las Redes Sociales de JUNJI como un canal de comunicación para uso a título personal.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 17 de 19

- b) Realizar comentarios ofensivos sobre funcionarios, autoridades de JUNJI o respecto de cualquier persona.
- c) Realizar respuestas ofensivas con ocasión de comentarios ciudadanos, inapropiados o no, que se plasmen en muros, historial, entre otros.
- d) Compartir las claves o acceso con terceros no autorizados.
- e) Omitir, borrar, inutilizar o no entregar las claves o acceso con ocasión del cambio de autoridades, feriado legal, licencias médicas, entre otros.

6.5 Recursos Restringidos de Internet

6.5.1 Instructivo para Solicitar Acceso a Recursos Restringidos de Internet

Cada vez que los funcionarios/as o usuarios/as de JUNJI que requieran acceder a sitios de internet bloqueados por motivos de su función deberán realizar una solicitud a cbs@junji.cl adjuntando un formulario de acceso autorizado por la jefatura o por el/la Subdirector/a Regional si fuese de una Dirección Regional.

Los funcionarios/as o usuarios/as de JUNJI deberán completar el Formulario de Solicitud de Acceso a Recursos Restringidos de internet o también llamado Formulario de Acceso a Páginas de Internet Bloqueadas, publicado en la intranet de JUNJI.

Una vez autorizado por la Jefatura de la Dirección Nacional o por el/la Subdirector/a Regional si fuese de una Dirección Regional, mediante la correspondiente firma del formulario, deberá adjuntarlo en un correo dirigido a cbs@junji.cl en la cual posteriormente de forma interna será derivado y podrá ser autorizado o rechazado por el/la Encargado/a de Ciberseguridad. Posteriormente, de ser autorizada la solicitud, será ejecutada por el personal de la **MDA**. Finalmente se notificará al funcionario el estado de resolución de la solicitud.

6.6 Gestión, Aplicación y Cumplimiento de la Política de Ciberseguridad

6.6.1 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, etc.

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET	PL-PL1515
		Versión N° 1
		Página 18 de 19

6.6.2 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.

6.6.3 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 presente política se encontrará publicada en la Intranet y el sitio www.junji.cl**, por lo tanto, se presume conocida por contratistas o adjudicatarios de servicios externos para todos los efectos legales.

6.6.4 Sanciones

El incumplimiento o violación debidamente acreditado de la presente Política, de las políticas específicas, procedimientos u otros documentos que se deriven de éstos, conlleva la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios/as de JUNJI, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente Política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones. Adicionalmente, dependiendo de la gravedad del incumplimiento del personal de JUNJI con respecto a la actual Política y procedimientos específicos relacionados, las Jefaturas podrán establecer una anotación de demérito.

6.6.5 Excepciones

La presente política, y las políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando, existan casos con razones fundadas, los cuales serán documentados por el/la Encargado/a de Ciberseguridad y debidamente autorizados por este o la Jefatura de Gabinete.

7 ANEXOS

Al presente documento se adjuntan los siguientes Anexos:

- PL-PL1515-Anexo N°1_Formulario Solicitud Cambio de Perfil

	POLÍTICA DE USO CORREO ELECTRÓNICO E INTERNET		PL-PL1515
			Versión N° 1
			Página 19 de 19

8 HISTORICO

Tabla N° 1: *Histórico de Modificaciones*

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