Subsecretaría para las Fuerzas Armadas

Gobierno de Chile

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES.

RESOLUCION EXENTA N° 8027

Santiago, 17 octubre 2025

VISTO:

a) DFL N°1/19.653, de 2001, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

b) La Ley Nº19.880, que establece Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado.

c) DFL N°29, de 2005, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N°18.834, sobre Estatuto Administrativo.

d) La Ley Nº20.424, Estatuto Orgánico del Ministerio de Defensa Nacional.

e) La Ley N°19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

f) La Ley Nº19.628, sobre protección de la vida privada.

g) La Ley Nº21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

h) La Ley Nº21.180, de Transformación Digital del Estado.

i) La Ley Nº21.464, modifica diversos cuerpos legales en materia de Transformación Digital del Estado.

j) La Ley Nº21.663, Marco de Ciberseguridad.

k) El Decreto Supremo N°83, de 2005, del Ministerio Secretaría General de la Presidencia, Aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

l) El Decreto Supremo N°164, de 2023, del Ministerio del Interior y Seguridad Pública, que aprueba Política Nacional de Ciberseguridad 2023-2028.

m) La Resolución Exenta N°8100, de 2018, que aprueba política general de seguridad de la información y revoca Resolución Exenta N°6180 de 2017, ambas de la Subsecretaría para las Fuerzas Armadas.

n) La Resolución Exenta N°8361, de 2019, de la Subsecretaría para las Fuerzas Armadas, que designa Encargado de Seguridad de la Información, Encargado de Ciberseguridad y Comité de Seguridad de la Información de la Subsecretaría para

las Fuerzas Armadas y deroga Resolución Exenta N°5952 del 04.ago.2015 y Resolución Exenta N°4412 del 22.jun.2017.

o) La Resolución N°36, de 2024, de la Contraloría General de la República, que fija normas sobre exención de toma de razón.

CONSIDERANDO:

1. Que, la revisión y análisis de la Política de Seguridad de la Información en las relaciones con los Proveedores corresponde a una tarea periódica, orientada al aseguramiento de la mejora continua del Sistema de Gestión de la Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas, conforme a las buenas prácticas de gestión establecidas en las normas internacionales en la materia.

2. Que, en el marco de dicha revisión, se ha determinado la necesidad de actualizar la Política de Seguridad de la Información en las relaciones con los Proveedores vigente, a fin de mantener un nivel acordado de seguridad de información asociados al uso de productos o servicios de proveedor.

3. Que, la entrada en vigor de las nuevas versiones de las normas internacionales en materia de Seguridad de la Información, en particular la norma ISO/IEC 27001:2022 y la norma ISO/IEC 27002:2022, así como su adopción oficial en Chile mediante la Norma Chilena NCh-ISO/IEC 27001:2023 y la NCh-ISO/IEC 27002:2022, exige que los objetivos de seguridad de la información en las funciones y niveles pertinentes deben ser objeto de seguimiento y de actualización periódica, a fin de garantizar su plena alineación con los estándares actualmente reconocidos.

4. Que, la Subsecretaría para las Fuerzas Armadas debe dar cumplimiento a las disposiciones legales y reglamentarias vigentes que regulan la Seguridad de la Información en los órganos de la Administración del Estado, en especial aquellas referidas a la protección de datos personales, la seguridad de los documentos electrónicos y la prevención de delitos informáticos.

5. Que, en la gestión institucional se han realizado cambios organizacionales y tecnológicos significativos que impactan directamente en la gestión de la Seguridad de la Información, lo cual refuerza la necesidad de contar con una política actualizada y acorde a la realidad operativa actual.

6. Que, en mérito de lo expuesto, resulta necesario actualizar la Política de Seguridad de la Información en las relaciones con los Proveedores.

RESUELVO:

1.- APRUÉBASE la Política de Seguridad de la Información en las relaciones con los Proveedores en la Subsecretaría para las Fuerzas Armadas, la que forma parte íntegra de la presente resolución.

2.- IMPLEMÉNTESE la presente Política de Seguridad de la Información en las relaciones con los Proveedores en la Subsecretaría para las Fuerzas Armadas, conforme a los roles y responsabilidades que en ella se asignan.

3.- DIFÚNDASE, la presente Política de Seguridad de la Información en las relaciones con los Proveedores a toda la comunidad funcionaria de la Subsecretaría para las Fuerzas

Armadas y a terceros que interactúen de manera habitual u ocasional con esta Subsecretaría de Estado.

4.- PUBLÍQUESE en la Intranet Institucional para conocimiento de toda la comunidad funcionaria.

5.- **DÉJESE SIN EFECTO** la Resolución Exenta N°8101, de 2018, de la Subsecretaría para las Fuerzas Armadas, en todo lo que dice relación con Políticas de Seguridad para las relaciones con los proveedores, manteniéndose vigentes las disposiciones sobre Política de Control de Acceso y Política de Dispositivos Móviles.

Anótese, comuníquese y archívese

Firmado por
Galo Mauricio
Eidelstein
Silber
Fecha
17/10/2025
16:16:12 CLST

GALO EIDELSTEIN SILBER
SUBSECRETARIO PARA LAS FUERZAS ARMADAS

MAP/RQR/MBA/DAI//MCP/JVC

Distribución
1. Gabinete MDN.
2. SS.FF.AA. Gabinete SS.FF.AA.
3. SS.FF.AA. Toda la Subsecretaría

Subsecretaría para las Fuerzas Armadas

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

Código:	SSFFAA-SSI-CSI-PP-02
Versión:	3.0
Fecha de la versión	21-08-2025
Creado por:	Mauricio Arancibia Pino
Visado por:	Juan Vásquez Carrasco
Nivel de confidencialidad:	Uso interno

Tabla de contenido

I. DECLARACIÓN INSTITUCIONAL

La Subsecretaría para las Fuerzas Armadas establece esta política con el propósito de asegurar un tratamiento adecuado de los activos de información en las relaciones con las y los proveedores. Esto incluye establecer y mantener controles que permitan gestionar de manera efectiva los riesgos asociados al intercambio de información, en conformidad con las normativas aplicables y los acuerdos establecidos.

Nota de confidencialidad

La información contenida en este documento es propiedad exclusiva de la Subsecretaría para las Fuerzas Armadas y está sujeta a políticas estrictas de confidencialidad. Su acceso, uso, reproducción o divulgación sin la debida autorización está estrictamente prohibido y podrá ser sancionado de acuerdo con las políticas internas de la Subsecretaría, así como con la legislación vigente en Chile sobre protección y seguridad de la información. Si usted ha recibido este documento por error, se solicita eliminarlo de inmediato y notificarlo a la Subsecretaría para las Fuerzas Armadas a la brevedad.

II. OBJETIVOS DE LA POLÍTICA

Definir directrices específicas para asegurar que las relaciones con proveedoras y proveedores externos cumplan con los estándares de seguridad de la información establecidos por la Subsecretaría para las Fuerzas Armadas. Este objetivo abarca la protección de los activos de información frente a riesgos asociados al acceso, manejo o almacenamiento de información, y busca garantizar la confidencialidad, integridad y disponibilidad de dichos activos durante toda la relación contractual.

III. DEFINICIONES

A continuación, se establecen las definiciones clave utilizadas en esta política:

- **Activo de Información**: Cualquier recurso tangible o intangible que contenga información relevante para la institución, incluyendo sistemas, datos, documentos y equipos tecnológicos.
- **Proveedor(a)**: Persona o entidad externa que, en virtud de un contrato o convenio, proporciona productos, servicios o soluciones a la institución.
- **Confidencialidad**: Propiedad de la información que asegura que solo las personas, procesos o sistemas autorizados puedan acceder a ella.
- **Integridad**: Propiedad que garantiza la exactitud y completitud de la información y de sus métodos de procesamiento.
- **Disponibilidad**: Propiedad que asegura que la información esté accesible y utilizable por una entidad autorizada cuando sea requerida.
- **Sistema de Gestión de Seguridad de la Información (SGSI)**: Marco para la gestión sistemática de los riesgos de seguridad de la información, diseñado para

preservar la confidencialidad, integridad y disponibilidad de los activos de información.

- **Riesgo de Seguridad de la Información**: Probabilidad de que una amenaza explote una vulnerabilidad, causando daño a los activos de información.
- **Contrato de Servicios**: Acuerdo formal entre la institución y el proveedor que define las condiciones bajo las cuales se ofrecen productos o servicios.

IV. ÁMBITO DE APLICACIÓN Y ALCANCE DE LA POLÍTICA

Esta política es aplicable a todas las relaciones contractuales entre la Subsecretaría para las Fuerzas Armadas y sus proveedores, incluyendo el personal externo que, en virtud de un contrato, tenga acceso a información, sistemas, recursos tecnológicos o instalaciones de la Subsecretaría. El alcance cubre todas las actividades relacionadas con el acceso, manejo, almacenamiento o procesamiento de información durante la prestación de servicios. Esto incluye, pero no se limita, a la implementación de medidas de seguridad, cumplimiento normativo y gestión de riesgos asociados a los activos de información involucrados.

V. MARCO NORMATIVO

Esta política se encuentra alineada con las disposiciones legales, normativas y estándares internacionales señalados en la **Política General de Seguridad de la Información** de la Subsecretaría para las Fuerzas Armadas.

En el marco de la gestión de proveedoras y proveedores, se considera especialmente relevante el cumplimiento de las siguientes normativas:

- **Ley Marco de Ciberseguridad (Ley N° 21.663/2024)**: Para la regulación de relaciones seguras y confiables con proveedoras y proveedores.
- **ISO/IEC 27002:2022 (Control 5.19)**: Sobre la seguridad de la información en las relaciones con proveedores.
- **Ley de Compras Públicas (Ley N° 19.886)**: Que regula las condiciones de contratación y las obligaciones de probidad, transparencia y cumplimiento normativo en los contratos públicos.
- **Normativa contractual interna**: Que regula las condiciones específicas de seguridad en la información para proveedoras y proveedores.

Esta política también incorporará cualquier normativa adicional aplicable que sea definida en futuras actualizaciones de la **Política General de Seguridad de la Información**

VI. GESTIÓN DE RIESGOS

En las relaciones con proveedoras y proveedores, se identificarán, evaluarán y gestionarán los riesgos asociados a la seguridad de la información. Estos riesgos

incluirán el acceso, manejo y almacenamiento de información, así como la continuidad de los servicios proporcionados.

La Subsecretaría aplicará procedimientos definidos en la **Política General de Seguridad de la Información** para garantizar que se adopten medidas proporcionales y efectivas que reduzcan la exposición a riesgos asociados con proveedoras y proveedores. Los riesgos identificados deberán ser revisados periódicamente y tratados mediante controles específicos definidos en los acuerdos contractuales.

VII. ROLES Y RESPONSABILIDADES

1. **Jefe/a del Servicio:**

- Responsable de aprobar esta política y de garantizar que su implementación esté alineada con los objetivos estratégicos de la Subsecretaría para las Fuerzas Armadas.

2. **Jefaturas de División:**

- Promover la aplicación de esta política en los procesos estratégicos y operacionales que involucren relaciones con proveedoras y proveedores.
- Velar por que los lineamientos de seguridad de la información se integren en las decisiones de contratación y en la supervisión de servicios externos.
- Apoyar al Comité de Seguridad de la Información en la identificación de riesgos transversales relacionados con proveedores, canalizando alertas o desviaciones detectadas en su ámbito de responsabilidad.

3. **Comité de Seguridad de la Información:**

- Supervisar la correcta aplicación de esta política.
- Revisar y proponer actualizaciones periódicas para asegurar su pertinencia frente a cambios normativos o tecnológicos.
- Coordinar las auditorías de cumplimiento relacionadas con los proveedores.
- Evaluar los incumplimientos relacionados con esta política, recomendando las acciones correctivas que correspondan y supervisando su implementación conforme a las normativas internas.

4. **Encargado/a de Seguridad de la Información:**

- Asesorar a las unidades de la Subsecretaría sobre los controles de seguridad aplicables a los proveedores.
- Verificar que los contratos con proveedores incluyan cláusulas de seguridad de la información acordes con la normativa vigente.
- Monitorear incidentes de seguridad relacionados con proveedores e implementar las acciones correctivas necesarias.

5. **Encargado/a de Ciberseguridad:**

- Colaborar en la identificación de riesgos tecnológicos asociados a los proveedores.
- Coordinar con proveedoras o proveedores medidas específicas para la protección de sistemas y datos críticos.

- Participar en la gestión de incidentes relacionados con accesos no autorizados o fallas en la infraestructura de los proveedores.

6. Jefaturas de Departamento:

- Garantizar que los procesos de contratación de proveedores en su área de responsabilidad incluyan la revisión de requisitos de seguridad de la información.
- Informar al Comité de Seguridad de la Información sobre cualquier incumplimiento detectado en el manejo de activos de información por parte de los proveedores.

7. Proveedores(as):

- Cumplir con las cláusulas de seguridad establecidas en los contratos firmados con la Subsecretaría.
- Informar oportunamente sobre cualquier incidente de seguridad que pueda comprometer los activos de información de la institución.
- Participar en auditorías o revisiones de cumplimiento cuando sean requeridas.

8. Personas usuarias internas relacionadas con proveedoras y proveedores:

- Asegurar que sus interacciones con proveedoras y proveedores cumplan con los lineamientos establecidos en esta política.
- Reportar cualquier actividad sospechosa o incidente relacionado con proveedoras y proveedores al Comité de Seguridad de la Información.

VIII. GESTIÓN DE ACTIVOS DE INFORMACIÓN

En el marco de las relaciones con proveedoras y proveedores, se identificarán y gestionarán los activos de información involucrados en los contratos. Esto incluye datos, sistemas, dispositivos y recursos tecnológicos que sean propiedad de la Subsecretaría para las Fuerzas Armadas y estén bajo el manejo de proveedoras y proveedores.

Las y los proveedores serán responsables de implementar las medidas de seguridad establecidas para proteger estos activos, conforme a las cláusulas contractuales y la normativa aplicable. La Subsecretaría verificará periódicamente el cumplimiento de estas disposiciones mediante auditorías y revisiones de cumplimiento.

IX. CIBERSEGURIDAD

En las relaciones con proveedoras o proveedores, se implementarán controles específicos para prevenir, detectar y mitigar ciberamenazas que puedan comprometer la seguridad de la información o la infraestructura tecnológica de la Subsecretaría para las Fuerzas Armadas.

Las y los proveedores estarán obligados a:

- Cumplir con las medidas de ciberseguridad estipuladas en los contratos, alineadas con la normativa vigente y los estándares internacionales aplicables.
- Notificar oportunamente cualquier incidente cibernético que afecte o pueda afectar los activos de información o sistemas de la Subsecretaría.

- Adoptar medidas preventivas, como mantener actualizados los sistemas utilizados en la prestación de servicios y proteger las credenciales de acceso a los sistemas institucionales.

La Subsecretaría realizará auditorías y revisiones periódicas para verificar el cumplimiento de estas medidas, asegurando que las y los proveedores mantengan un nivel adecuado de ciberseguridad. Además, se fomentará la cooperación entre la Subsecretaría con las y los proveedores para mejorar continuamente las capacidades frente a amenazas emergentes.

X. DIFUSIÓN DE LA POLÍTICA

El **Comité de Seguridad de la Información** será responsable de coordinar la difusión de esta política, asegurando que, a través del Encargado de Seguridad de la Información todas las personas proveedoras y el personal interno comprendan y apliquen sus disposiciones. Para ello, se garantizará el acceso a la versión más actualizada de la política a través de la intranet institucional, el correo electrónico y documentos entregados durante los procesos de contratación. Además, se organizarán capacitaciones periódicas dirigidas especialmente a los equipos que supervisan y gestionan a las y los proveedores, con el objetivo de reforzar el entendimiento y cumplimiento de las disposiciones de seguridad.

XI. MEDIDAS DISCIPLINARIAS Y NORMAS CONTRACTUALES ANTE INCUMPLIMIENTO DE OBLIGACIONES

El incumplimiento de las disposiciones establecidas en esta política ya sea por parte de las y los proveedores o del personal interno relacionado con la gestión de proveedoras y proveedores, será evaluado según su gravedad y las consecuencias que genere para la seguridad de la información de la Subsecretaría.

Las medidas disciplinarias aplicables incluyen:

- **Para proveedoras y proveedores**:
    - Aplicación de cláusulas de multas definidas en los contratos.
    - Suspensión temporal o termino anticipado del contrato por incumplimientos graves.
    - Inclusión en un registro institucional de proveedoras y proveedores con restricciones para futuros procesos de contratación.
- **Para personal interno**:
    - Aplicación de medidas administrativas conforme al Estatuto Administrativo y las normativas internas vigentes.

XII. EVALUACIÓN Y AUDITORÍA

La implementación de esta política será objeto de evaluaciones periódicas para verificar su efectividad y alineación con las normativas vigentes y los estándares de seguridad de la información aplicables.

El **Comité de Seguridad de la Información** supervisará estas actividades y garantizará que los resultados permitan adoptar medidas de mejora continua, fortaleciendo la gestión de la seguridad en las relaciones con proveedoras y proveedores.

ACTUALIZACIÓN DE LA POLÍTICA

Esta política será revisada periódicamente para asegurar su alineación con los objetivos estratégicos de la Subsecretaría para las Fuerzas Armadas y las normativas vigentes aplicables.

El **Comité de Seguridad de la Información** será responsable de coordinar las actualizaciones, considerando los cambios en el entorno normativo, los riesgos emergentes y las necesidades operativas. Todas las modificaciones serán aprobadas siguiendo los procedimientos internos establecidos y comunicadas oportunamente a las y los proveedores y al personal interno involucrado.

XIII. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
Versión	**Fecha**	**Autor**	**Descripción**
1.0	15.09.2017	Mauricio Arancibia Pino	Elaboración inicial
2.0	10.12.2018	Mauricio Arancibia Pino	Aplicación de formato, ámbitos, definiciones, disposiciones de la política
3.0	25.11.2024	Comité de Seguridad de la Información	Revisión completa, cambios normativos y aplicación de nueva estructura