

APRUEBA POLÍTICAS ESPECÍFICAS DE
 SEGURIDAD, POLÍTICA DE SEGURIDAD PARA
 LAS RELACIONES CON LOS PROVEEDORES,
 POLÍTICA DE CONTROL DE ACCESO Y
 POLÍTICA DE DISPOSITIVOS MÓVILES Y
 REVOCA RESOLUCIÓN EXENTA N° 6181 DE
 FECHA 21.SEP.2017 DE LA SUBSECRETARÍA
 PARA LAS FUERZAS ARMADAS.



SANTIAGO, 14 DIC 2018

RESOLUCIÓN EXENTA N° 8101

MINISTERIO DE HACIENDA
 OFICINA DE PARTES
RECIBIDO

CONTRALORÍA GENERAL
 TOMA DE RAZÓN
RECEPCION

DEPARTO JURÍDICO		
DEPARTO YACIMIENTO		
DEPARTO CONTABLE		
SUBDEPARTAMENTO GENERAL		
SUBDEPARTAMENTO CUENTAS		
SUBDEPARTAMENTO CIVIL Bienes Nac.		
DEPARTO ADMINISTRACIÓN		
DEPARTO VOP. U y T		
SUBDEPARTAMENTO MUNICIPAL		

REFRENDACION
 REFERENCIAL: _____
 IMPRIMIDA: _____
 ANOTADA: _____
 REVISADA: _____
 FECHA: _____

JFGB/BH/ MAP

VISTOS:

- DFL N° 1/19.653, de 2001, que fijó el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, artículo 5.
- Ley N° 19.880, que establece Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado.
- Ley N° 20.424, sobre Estatuto Orgánico del Ministerio de Defensa Nacional, artículo 21, letras c) y o).
- DFL. N° 29, de 2004, que Fija Texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo;
- Ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley N° 19.628, sobre "Protección de Vida Privada".
- Ley N° 19.223, sobre "Delitos Informáticos".
- Ley N° 20.285, sobre "Acceso a la Información Pública".
- Decreto Supremo N° 83 de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos.
- Decreto Supremo N° 93 de 2006, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los Órganos de la Administración del Estado y de sus Funcionarios.
- Decreto Supremo N° 134 de 2006, del Ministerio Secretaría General de la Presidencia, que Declara derogado el Decreto N° 26 de 2001, Reglamento sobre el secreto o reserva de los actos y documentos de la Administración Del Estado.
- Decreto Supremo N° 158 de 2007 del Ministerio Secretaría General de la Presidencia, que Modifica Decreto Supremo N° 81, de 2004, Que aprueba norma técnica para los Órganos de la Administración Del Estado sobre interoperabilidad de documentos electrónicos.
- Resolución Exenta N° 7.758 de fecha 04 de octubre de 2013 que Actualiza Política de Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas.
- Resolución Exenta N° 6.849 de fecha 03 de octubre de 2016 que amplía Resolución Exenta N° 7.758 de 04 de octubre de 2013, que aprueba Política de Seguridad de la Información.
- Resolución Exenta N° 6180 de fecha 21 de septiembre de 2017, que aprueba Política de Seguridad de la Información y deroga resoluciones anteriores.
- Resolución Exenta N° 5.952 de fecha 04 de agosto de 2015, que Designa Encargado de Seguridad de la Información, Comité de Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas.
- Resolución Exenta N° 4.412 de fecha 22 de junio de 2017, que Modifica Resolución Exenta N° 5.952 de fecha 04 de agosto de 2015.

- r) Resolución N°1.600, de 2008, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.
- s) Decreto Exento N°290, del 25 de agosto de 2016, del Ministerio de Hacienda, que aprueba Programa Marco de los Programas de Mejoramiento de la Gestión de los Servicios en el año 2017.
- t) Decreto Exento N°297, del 08 de agosto de 2017 del Ministerio de Hacienda, que aprueba Programa Marco de los Programas de Mejoramiento de la Gestión de los Servicios en el año 2018.
- u) Decreto Exento N°324, del 19 de octubre de 2018, del Ministerio de Hacienda, que aprueba Programa Marco de los Programas de Mejoramiento de la Gestión de los Servicios en el año 2019.

CONSIDERANDO:

1. Que la revisión y análisis de la Política General de Seguridad de la Información corresponde a una tarea periódica, orientada al aseguramiento de la mejora continua del sistema, establecida en el Plan de Trabajo realizado por el Comité de Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas.
2. Que, dentro de los objetivos estratégicos vigentes de la Subsecretaría para las Fuerzas Armadas, se encuentra el garantizar la plena seguridad de los activos de información en su confidencialidad, integridad y disponibilidad mejorando continuamente la gestión de los procesos críticos institucionales.
3. Que la Subsecretaría para las Fuerzas Armadas, debe cumplir con las normas que regulan los procedimientos de Seguridad de la Información, de conformidad con los requisitos establecidos en la Norma Chilena NCH - ISO 27.001:2013 y en el Decreto Supremo N°83, de 2005, que aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
4. Que, en la gestión institucional se han producido cambios significativos que impactan directamente a la Política General de Seguridad de la Información.

RESUELVO:

1. **APRÚEBASE**, la Políticas Específicas de Seguridad de la Información, Política de Seguridad para las Relaciones con los Proveedores, Política de Control de Acceso y Política de Dispositivos Móviles, anexas al presente acto administrativo.
2. **IMPLEMENTÉSE**, las políticas que por este acto se aprueban, por parte del Comité de Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas, conforme a los roles que en ella se asignan.
3. **DIFÚNDASE**, las políticas que se adjuntan al presente acto administrativo, a los funcionarios de Planta, Contrata, a Honorarios, funcionarios de las Fuerzas Armadas destinados a prestar servicios en

esta Institución y a los terceros que interactúen de manera habitual u ocasional con esta Subsecretaría.

4. **REVÓCASE**, a contar de la total tramitación de la presente resolución, la Resolución Exenta N°6.181 de 2017, por medio de la cual, fue aprobada la anterior Política de Seguridad de la Información para las relaciones con los proveedores y Política Específica de Seguridad de la Información.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

FDO.) JUAN FRANCISCO GALLI BASILI, Subsecretario para las Fuerzas Armadas, lo que transcribo para su conocimiento, Juan Ibacache Ibacache, Jefe División Administrativa, Subsecretaría para las Fuerzas Armadas.




JUAN IBACACHE IBACACHE
Jefe de la División Administrativa
SUBSECRETARÍA PARA LAS FUERZAS ARMADAS

JFGB/JII/MAP

DISTRIBUCIÓN:

1. Gabinete Sr. Subsecretario para las Fuerzas Armadas
2. Jefe de División Administrativa
3. Jefe de División de Asuntos Institucionales
4. Jefa de División de Auditoría
5. Jefe de División de Presupuesto y Finanzas
6. Jefe de División Jurídica
7. Unidad de Planificación y Control de Gestión
8. Comité de Seguridad de la Información
9. Encargado de Seguridad de la Información (Archivo)



POLÍTICA DE SEGURIDAD PARA LAS RELACIONES CON LOS PROVEEDORES

SUBSECRETARÍA PARA LAS FUERZAS ARMADAS



**Versión 2.0
Diciembre 2018**



ÍNDICE

I	DECLARACIÓN INSTITUCIONAL.....	3
II	OBJETIVO	3
III	ALCANCE.....	3
IV	DOCUMENTOS DE REFERENCIA	3
V	ROLES Y RESPONSABILIDADES.....	4
VI	DEFINICIONES.....	5
VII	POLITICA	5
VIII	DIFUSIÓN DE LA POLÍTICA.....	9
IX	MEDIDAS DISCIPLINARIAS	9
X	PERIODICIDAD DE EVALUACIÓN Y REVISIÓN	9
XI	APROBACIÓN.....	10
XII	CONTROL DE CAMBIOS	11

I DECLARACIÓN INSTITUCIONAL

La Subsecretaría para las Fuerzas Armadas establece como "Política de seguridad de la información para las relaciones con los proveedores", un conjunto de directrices enfocadas en la contratación de servicios externos a fin de controlar y proteger los activos de información del Servicio que tengan acceso los proveedores.

II OBJETIVO

Establecer el marco normativo para la contratación de servicios externos, en relación a la seguridad de la información, para los proveedores de la Subsecretaría para las Fuerzas Armadas y todo el personal externo que trabaja en la Institución y que, en el desarrollo de sus funciones, pueda tener acceso a información, sistemas de información o recursos de la Subsecretaría en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información.

III ALCANCE

Todas las actividades desarrolladas en la Subsecretaría por personal que presta servicios para esta organización y que pertenece a empresas proveedoras de servicios, vinculadas a través del correspondiente contrato de prestación de servicios.

Esta política abarca los siguientes controles definidos en la norma NCh-ISO-27001:2013 A.15.01.01 Políticas de Seguridad de la Información para las relaciones con los proveedores.

IV DOCUMENTOS DE REFERENCIA

- Política general de seguridad de la información.
- Políticas específicas de seguridad de la información.
- Instructivo de elaboración de documentos.
- Ley N° 20.424 Estatuto Orgánico del Ministerio de Defensa Nacional.
- D.S. N° 248 de 2010, Reglamento Orgánico y de Funcionamiento del Ministerio de Defensa Nacional.
- Ley 19.628 Sobre la protección de la vida privada, Ministerio Secretaría General de la Presidencia.
- Ley 20.285 Sobre acceso a la información pública, Ministerio Secretaría General de la Presidencia.
- Ley 19.223 Sobre figuras penales relativas a la informática.
- Ley 19.886 Ley de Compras Públicos y su Reglamento.

V ROLES Y RESPONSABILIDADES

Subsecretario(a) para las Fuerzas Armadas:

Responsable de aprobar la “Política de Dispositivos Móviles” de la Subsecretaría para las Fuerzas Armadas y sus modificaciones, con la asistencia del Comité de Seguridad de la Información.

Comité de Seguridad de la Información:

- Será el responsable de supervisar la implementación de procedimientos y estándares que se desprendan de la presente “Política de seguridad de la información para las relaciones con los proveedores”.
- Propondrá estrategias y soluciones específicas para la implantación de los controles necesarios para velar por el fiel cumplimiento de la política.
- Concientizar a los usuarios sobre la aplicación de la política.
- Proponer actualización de la política, revisar anualmente la política.
- Difundir la política a través de los medios disponibles de la Institución.
- Arbitrar conflictos en materia de seguridad de la información relacionada con la presente política.

Encargado(a) de Seguridad de Información:

- Supervisar el cumplimiento de la presente política.
- Coordinar revisiones periódicas en el cumplimiento de la presente política.
- Asesora en materia de seguridad de la información a la autoridad de la Subsecretaría para las Fuerzas Armadas y a los integrantes del Comité de Seguridad de la Información.

División de Presupuesto y Finanzas:

- Velar por el cumplimiento de la siguiente política y de la inclusión de las cláusulas de confidencialidad en contratos con terceros.

Proveedores:

Dar estricto cumplimiento a las normas de seguridad de la información descritas en la presente política, en la documentación del Sistema de Gestión de Seguridad de la Información y en los Contratos y Resoluciones firmadas por la autoridad competente de la Subsecretaría para las Fuerzas Armadas.”

Personal Externo que presta servicios para la Subsecretaría:

Dar estricto cumplimiento a las normas de seguridad descritas en la presente política y en la documentación del Sistema de Gestión de Seguridad de la Información de esta Subsecretaría.

Usuarios

Todo el personal de la Subsecretaría que interactúa con el personal de los proveedores debe dar estricto cumplimiento a la reglamentación dispuesta por la autoridad superior sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de la organización.

VI DEFINICIONES

Sistema de Gestión de Seguridad de la información (SGSI):

Es un conjunto de procesos para gestionar eficientemente el acceso a la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información.

NCh-ISO 27001:

Norma Chilena de Seguridad de la Información, traducción de la norma internacional ISO 27001.

VII POLÍTICA

a) Cumplimiento de la Política General de la Seguridad de la Información

Todo el personal externo que desarrolle labores para la Subsecretaría deberá tomar conocimiento de la Política General de Seguridad de la Información, observando sus directrices y colaborando en su aplicación dentro de su ámbito de acción.

Para estos efectos, el trabajo o proyecto realizado por el proveedor debe ser compatible con los estándares de seguridad de la información establecidos por esta Subsecretaría.

b) Prestación de servicios en la Subsecretaría para las Fuerzas Armadas

Los proveedores sólo podrán desarrollar para la Subsecretaría aquellas actividades cubiertas bajo el correspondiente contrato de prestación de servicios y de acuerdo a lo establecido en las correspondientes bases y contrato de prestación de servicios.

La empresa proveedora deberá asegurar que todo su personal que presta servicios en la Subsecretaría para las Fuerzas Armadas, tiene la formación y capacitación para efectuar el servicio contratado. Asimismo, a tomar

conocimiento y comprometerse a cumplir con las Políticas de Seguridad de la Información.

c) Confidencialidad de la Información

El personal externo que tenga acceso a información de la Subsecretaría entenderá que dicha información por defecto, tiene el carácter de confidencial.

Queda prohibido para los proveedores revelar, modificar, destruir o dar mal uso de la información, cualquiera que sea el soporte de la información.

El proveedor deberá resguardar por un tiempo indefinido la confidencialidad y no podrá difundir la información a la que se tiene acceso, salvo que esté debidamente autorizado por el dueño de esta.

El proveedor deberá minimizar el número de informes en formato papel que contengan información confidencial o de uso interno y se mantendrán los mismos en un lugar seguro y fuera del alcance de terceros (de acuerdo a lo establecido en la Política de pantalla y escritorios limpios).

En caso de que, por motivos directamente relacionados con el trabajo, el empleado de la empresa proveedora de servicios tome conocimiento de información confidencial contenida en cualquier tipo de soporte, deberá entender que es estrictamente temporal, con obligación de secreto y sin que con ello se le confiera derecho de posesión, titularidad o copia sobre la citada información.

Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para la Subsecretaría.

El incumplimiento de estas será sancionado en los términos establecidos por las leyes vigentes.

d) Propiedad Intelectual

El personal externo deberá garantizar el cumplimiento de las restricciones legales de uso del material protegido por normas de propiedad intelectual.

Queda estrictamente prohibido el uso de programas informáticos que no cuenten con licencia original y vigente.

Queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.

e) Intercambio de Información

Durante el intercambio de información, ninguna persona debe ocultar o manipular su identidad bajo ninguna circunstancia.

En relación al intercambio de información dentro del marco del contrato de prestación de servicios, se considerarán no autorizadas las siguientes actividades:

- Trasmisión o recepción de toda clase de material pornográfico, mensajes de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaraciones o mensaje clasificable como ofensivo o ilegal.
- Trasmisión o recepción de material protegido de Copyright infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de material referido a campañas políticas.
- Trasmisión de avisaje comercial, material que tenga como propósito el tráfico de influencias y el uso de información privilegiada.
- Material relacionado con promoción de la prostitución infantil y el terrorismo.
- Cualquier forma de acoso laboral, sexual, discriminación en cualquiera de sus formas y violencia de género.

f) Uso apropiado de recursos

Los recursos que la Subsecretaría pone a disposición del personal externo, están disponibles exclusivamente para cumplir las obligaciones y propósitos operativos para los cuales fueron proporcionados. La Subsecretaría se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

Cualquier información introducida a la red de la Subsecretaría o cualquier equipo conectada a ella a través de soportes automatizados, internet, correo electrónico, o cualquier otro medio, deberá cumplir los requisitos establecidos en las Políticas de Seguridad de la Información de la Subsecretaría, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.

Se prohíbe expresamente:

- La comercialización o entrega de información de propiedad de la Subsecretaría o bases de datos de usuarios, personal y/o proveedores.
- El uso de los recursos proporcionados por la Subsecretaría para actividades no relacionadas con el propósito del servicio.
- Introducir en los Sistemas de Información o la Red de la Subsecretaría contenidos obscenos, amenazadores, inmorales u ofensivos.

- Introducir voluntariamente a la red de la Subsecretaría cualquier tipo de malware (programas, macros, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencias de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Todo personal con acceso a la red de la Subsecretaría tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los sistemas de elementos destinados a destruir o corromper los datos informáticos.
- Intentar obtener sin autorización explícita otros derechos o accesos que la Subsecretaría le haya asignado.
- Intentar acceder sin autorización explícita a áreas restringidas de los sistemas de información de la Subsecretaría.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, dañar o alterar los recursos informáticos de la Subsecretaría.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos de responsabilidad y custodia de la Subsecretaría.

g) Responsabilidad del proveedor

Los proveedores de servicios deberán asegurarse de que todo el personal que desarrolla labores para la Subsecretaría, respete las siguientes condiciones en el desarrollo de sus actividades informáticas:

- Las personas con acceso a la información de la Subsecretaría son responsables de la actividad desarrollada por su identificador de usuario y todo lo que dé él se derive.
- Los usuarios no deberán utilizar ningún identificador distinto al propio, aunque disponga de la autorización del propietario.

h) Equipamiento del proveedor

Los proveedores de servicios deberán asegurarse de que todo el equipamiento informático utilizado para acceder a información de responsabilidad de la Subsecretaría cumpla las siguientes normas:

- Cuando se desatienda un puesto durante un periodo corto de tiempo el sistema deberá activar su bloqueo en forma manual o automática.
- Ningún equipo dispondrá de herramientas que puedan transgredir el sistema de seguridad ni las autorizaciones dentro de los sistemas de la organización.
- El equipo debe mantenerse de acuerdo a las especificaciones del fabricante.
- Todos los equipos del usuario estén adecuadamente protegidos frente a malware y virus computacionales.

VIII DIFUSIÓN DE LA POLÍTICA

Es de suma importancia y resulta clave para que la presente política se integre en la cultura organizacional de la Subsecretaría para las Fuerzas Armadas, la existencia de un plan formal de difusión que estará bajo la responsabilidad del Comité de Seguridad de la Información, para lo cual se establece como medio de comunicación, el sitio web institucional, el correo electrónico y el contenido del Sistema de Seguridad de la Información dispuesto en la Intranet institucional, además del apoyo de los Jefes de Divisiones y Departamento.

El personal de planta, contrata, honorarios, funcionarios de las Fuerzas Armadas destinados a prestar servicio y personal de servicios externos, tendrán acceso a esta política, en su última versión, vía Web Institucional para su uso externo e Intranet Institucional bajo el link "Seguridad de la Información" donde accederá al contenido del Sistema de Seguridad de la Información, creado para difundir todas la políticas y procedimientos que surjan del Comité de Seguridad de la Información en forma interna.

Con el objeto de lograr un buen entendimiento de la Política, se organizarán charlas de difusión dirigida a los funcionarios de la Institución.

IX MEDIDAS DISCIPLINARIAS

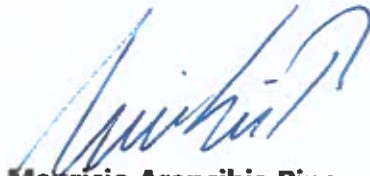
El personal de la Subsecretaría para las Fuerzas Armadas, incurrirá en responsabilidad administrativa o su equivalente cuando vulneren o contravengan la presente Política, la que deberá ser acreditada mediante una investigación sumaria o la medida administrativa que corresponda, la cual tendrá por objeto verificar la existencia de los hechos, y la individualización de los responsables y su participación, si la hubiera.

X PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

Uno de los pilares que sustenta la Política de Seguridad de la Información para las relaciones con el proveedor, es la mejora continua del documento. Al respecto, el Comité de Seguridad de la Información reevaluará la Política de Seguridad para las relaciones con el proveedor cada 2 años. Asimismo, efectuará toda modificación cuando se produzcan cambios significativos que la impacten.

XI APROBACIÓN

Elaborado por



Mauricio Arancibia Pino

Encargado de Seguridad de la Información
Subsecretaría para las Fuerzas Armadas


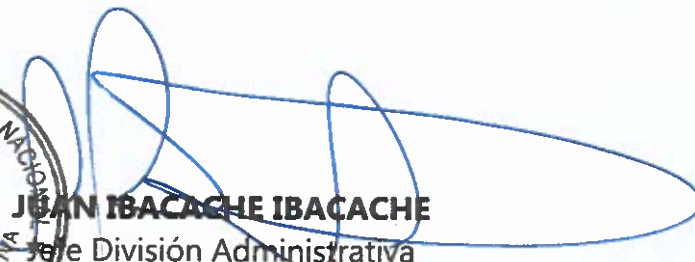
Visado por



Sergio Pizarro Flores

Jefe Departamento Adquisiciones
Subsecretaría para las Fuerzas Armadas

Visado por



JUAN IBACACHE IBACACHE

Jefe División Administrativa
Subsecretaría para las Fuerzas Armadas

Aprobada por



JUAN FRANCISCO GALLI BASILI
Subsecretario para las Fuerzas Armadas
Ministerio de Defensa Nacional

XII CONTROL DE CAMBIOS

CONTROL DE CAMBIOS DEL DOCUMENTO				
N° versión	Fecha	Motivo modificación	Páginas elaboradas y/o modificadas	Autor
1.0	15.09.2017	Elaboración inicial	Todas	Mauricio Arancibia P.
2.0	10.12.2018	Cambio de formato	Todas	Mauricio Arancibia P.