Subsecretaría para las Fuerzas Armadas

Gobierno de Chile

MINISTERIO DE DEFENSA NACIONAL
SUBSECRETARÍA FF.AA.
27 NOV 2017
TOTALMENTE TRAMITADA

MINISTERIO DE HACIENDA
OFICINA DE PARTES

R E C I B I D O

CONTRALORÍA GENERAL
TOMA DE RAZON

R E C E P C I O N

DEPART JURIDICO		
DEP T.R. Y REGISTRO		
DEPART CONTABIL		
SUB DEPTO C CENTRAL		
SUB DEPTO E CUENTAS		
SUB DEPTO CPV Bienes Nac.		
DEPART AUDITORIA		
DEPART V OP U y T		
SUB DEPTO MUNICIP		

REFRENDACION

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES Y POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN

SANTIAGO, 21 SEP 2017

RESOLUCIÓN EXENTA Nº 6181

VISTOS:

a) Lo dispuesto en el Art. 5 del DFL Nº 1/19.653, de 2001, que fijó el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

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

c) Ley Nº20.424, sobre Estatuto Orgánico del Ministerio de Defensa Nacional.

d) El DFL. Nº29, de 2004, que Fija Texto refundido, coordinado y sistematizado de la Ley Nº18.834, sobre Estatuto Administrativo;

e) Ley Nº19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

f) Ley Nº19.628, sobre Protección de Vida Privada.

g) Ley Nº19.223, sobre Delitos Informáticos.

h) Ley Nº 20.285, sobre Acceso a la Información Pública.

i) Decreto Supremo Nº 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.

j) Decreto Supremo Nº 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 Funcionario.

k) Decreto Supremo Nº 134 de 2006, del Ministerio Secretaría General de la Presidencia, que Declara derogado el Decreto Nº 26 de 2001, Reglamento sobre el secreto o reserva de los actos y documentos de la Administración Del Estado

l) Decreto Supremo Nº 158 de 2007 del Ministerio Secretaría General de la Presidencia, que Modifica Decreto Supremo Nº 81, de 2004, Que aprueba norma técnica para los Órganos de la Administración Del Estado sobre interoperabilidad de documentos electrónicos.

m) Resolución Exenta Nº 7.758 de fecha 04 de octubre de 2013 que Actualiza Política de Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas.

GRR/GRM/MAP

201721274

n) Resolución Exenta Nº 6.849 de fecha 03 de octubre de 2016 que amplia Resolución Exenta Nº 7.758 de 04 de octubre de 2013, que aprueba Política de Seguridad de la Información.

o) Resolución Exenta Nº 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.

p) Resolución Exenta Nº 4.412 de fecha 22 de junio de 2017, que Modifica Resolución Exenta Nº 5.952 de fecha 04 de agosto de 2015.

q) Resolución Nº1.600, de 2008, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

r) Decreto Exento Nº290, 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.

s) Decreto Exento Nº297, del 08 de agosto 2017 del Ministerio de Hacienda, que aprueba Programa Marco de los Programas de Mejoramiento de la Gestión de los Servicios en el año 2018.

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 del Comité de Seguridad de la Información.

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 Nº83, 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 las Políticas de Seguridad de la Información.

5. Que, las Políticas de Seguridad de la Información, se encuentran aprobada por el Comité de Seguridad de la Información con fecha 15 de Septiembre de 2017, según consta en Acta de la fecha indicada.

R E S U E L V O:

1. **APRÚEBESE**, la Política de Seguridad de la Información para las Relaciones con los Proveedores y Política Específica de Seguridad de la Información, en conformidad a las directrices emanadas del Comité de Seguridad de la Información.

2. **IMPLEMÉNTESE,** las presentes políticas por el Comité de Seguridad de la Información, conforme a los roles que se les ha asignado y para todo el personal de la Subsecretaría de las Fuerzas Armadas.

3. **DIFÚNDASE,** las presentes Política de Seguridad de la Información para las Relaciones con los Proveedores y Política Específica de Seguridad de la Información, que se adjunta en este acto y todo instrumento relacionado con esta materia, a los funcionarios de Planta, Contrata, a Honorarios, funcionarios de las Fuerzas Armadas, destinados a prestar servicio en esta institución y a los terceros que interactúen de manera habitual u ocasional con esta Subsecretaría.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

POR ORDEN DE LA SRA SUBSECRETARIA PARA LAS FUERZAS ARMADAS

MINISTERIO DE DEFENSA NACIONAL
DIVISIÓN ADMINISTRATIVA
SS.FF.AA.

GONZALO REBOLLEDO RODRÍGUEZ
JEFE DIVISIÓN ADMINISTRATIVA
SUBSECRETARIA PARA LAS FUERZAS ARMADAS
MINISTERIO DE DEFENSA NACIONAL

GRR/GRM/MAP

201721274

DISTRIBUCIÓN:

1. Gabinete Sra. Subsecretaria de las Fuerzas Armadas
2. Jefe de División Administrativa
3. Jefe de División de Asuntos Institucionales
4. Jefa de División de Auditoria
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
10. Archivo

Subsecretaría para las Fuerzas Armadas

Gobierno de Chile

2017

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

SUBSECRETARÍA PARA LAS FUERZAS ARMADAS

Versión 1.0
Septiembre 2017

INDICE

I. DECLARACIÓN INSTITUCIONAL

La Subsecretaría para las Fuerzas Armadas establece como "Políticas 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 Subsecretaria 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 Subsecretaria 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 Subsecretaria 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 el proveedor.

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 Secretaria General de la Presidencia.
- Ley 20.285 Sobre acceso a la información pública, Ministerio Secretaria 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

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 Internos: 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

SGSI: Sistema de Gestión de Seguridad de la información, 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

Malvare: es un tipo de software o programa computacional que tiene como objetivo infiltrarse o dañar un computador o sistema de información.

VII. POLITICA

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

Todo el personal externo que desarrolle labores para la Subsecretaria 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 este 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 privado y se mantendrán los mismos en un lugar seguro y fuera del alcance se 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 explicita, 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 Subsecretaria pone a disposición del personal externo, están disponibles exclusivamente para cumplir las obligaciones y propósitos operativos para los cuales fueron proporcionados. La Subsecretaria 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 Subsecretaria.
- 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.
- Las personas con acceso a información con responsabilidad de la Subsecretaría deberán seguir las siguientes directrices en relación a la gestión de las contraseñas.
- Seleccionar contraseñas de calidad.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Cambiar las contraseñas periódicamente y evitar reutilizar o reciclar contraseñas antiguas.
- Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión ("login").
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar cualquier incidente de seguridad relacionado con sus contraseñas como perdidas, robos o indicio de perdida de confidencialidad.
- Cualquier persona con acceso a información de responsabilidad de la Subsecretaria deberá velar para que los equipos queden protegidos, cuando vayan a quedar desatendidos (ver Política de pantallas y escritorios limpios).

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 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.

VIII. DIFUSIÓN

La responsabilidad de la difusión de la Política General de Seguridad de la Información para las relaciones con el proveedor al interior del Servicio, es del Comité de Seguridad de la Información, para lo cual se establece como medio de comunicación, el correo electrónico y el sitio web elaborado y dispuesto por el Comité de Seguridad de la Información, así como el apoyo de los Jefes/as de Divisiones y Departamentos.

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 Intranet Institucional y/o el sitio web del Sistema de Seguridad de la Información, creado para difundir todas las Políticas y Procedimientos que surjan del Comité de Seguridad de la Información.

El personal de empresas externas, tendrán acceso a esta Política, en su última versión, a través del Departamento de Adquisiciones de esta Subsecretaría.

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

IX. MEDIDAS DISCIPLINARIAS

De acuerdo a lo establecido en las cláusulas asociadas en los contratos de prestación de servicios, todo el personal externo que desarrolle labores para esta Subsecretaría deberá cumplir con lo establecido en este documento y en las políticas y procedimientos del Sistema de Seguridad de la Información. En caso de incumplimiento de cualquiera de estas obligaciones, la Subsecretaría se reserva el derecho a veto sobre el personal que haya cometido la infracción, así como las sanciones que se consideren pertinentes en relación a la empresa o persona contratada.

X. FORMATO DE LA POLÍTICA

El formato utilizado para la elaboración de las políticas y las que emerjan, es el utilizado para elaborar todas las políticas que resulten del trabajo del Comité de Seguridad de la Información, cuyo formato se encuentra en el:

- Instructivo de Elaboración de Documentos

XI. ACTUALIZACIÓN

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 anualmente. Asimismo, efectuará toda modificación cuando se produzcan cambios significativos que la impacten.

XII. APROBACIÓN

Elaborado por

Mauricio Arancibia Pino
Encargado de Seguridad de la Información
Subsecretaría para las Fuerzas Armadas

Revisado por

Patricio Inostroza Hernández
Jefe Departamento Adquisiciones
Subsecretaría para las Fuerzas Armadas

Gustavo Ruz Muñoz
Jefe Unidad Planificación y Control de Gestión
Subsecretaría para las Fuerzas Armadas

Visado por

GONZALO REBOLLEDO RODRÍGUEZ
Jefe División Administrativa
Subsecretaría para las Fuerzas Armadas

Aprobada por

PAULINA VODANOVIC ROJAS
Subsecretaria para las Fuerzas Armadas
Ministerio de Defensa Nacional

XIII. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS DEL DOCUMENTO				
Nº versión	Fecha	Motivo modificación	Páginas elaboradas y/o modificadas	Autor

1.0	15.09.2017	Elaboración inicial	Todas	Mauricio Arancibia P.