Subsecretaría para las Fuerzas Armadas

Gobierno de Chile

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		
DEPTO. Y REGISTRO		
DEPART. CONTABIL.		
SUB DEPTO. C.CENTRAL		
SUB DEPTO. E.CUENTAS		
SUB DEPTO. C.P.Y. Bienes Nac.		
DEPART. AUDITORIA		
DEPART. V.O.P. U. y T.		
SUB DEPTO. MUNICIP.		

REFRENDACION

REFRENDACION $_____
DECRETO _____
ANTERIOR _____
IMPUTACION _____

MINISTERIO DE DEFENSA NACIONAL
SUBSECRETARIA FF.AA.

24 DIC 2018

TOTALMENTE TRAMITADA

APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y REVOCA RESOLUCIÓN EXENTA Nº 6180 DE FECHA 21.SEP.2017 DE LA SUBSECRETARÍA PARA LAS FUERZAS ARMADAS.

SANTIAGO, 14 DIC 2018

RESOLUCIÓN EXENTA Nº 8100

VISTOS:

a) 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, artículo 5.

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, artículo 21, letras c) y o).

d) 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 Funcionarios.

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.

n) Resolución Exenta Nº 6.849 de fecha 03 de octubre de 2016 que amplia Resolución Exenta Nº7.758 de 04 de octubre de 2013, que aprueba Política de Seguridad de la Información.

o) Resolución Exenta Nº 6180 de fecha 21 de septiembre de 2017, que aprueba Política de Seguridad de la Información y deroga resoluciones anteriores.

p) 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.

q) 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.

JFGB/JII/MAP

-

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

s) 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.

t) Decreto Exento Nº297, 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 Nº324, 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 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 la Política General de Seguridad de la Información.

R E S U E L V O:

1. **APRÚEBASE**, la Política General de Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas, anexa al presente acto administrativo.

2. **IMPLEMÉNTESE,** la política que por este acto se aprueba, 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**, la presente Política General de Seguridad de la Información, que se adjunta 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 Nº6.180 de 2017, por medio de la cual, fue aprobada la anterior Política 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.

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

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)

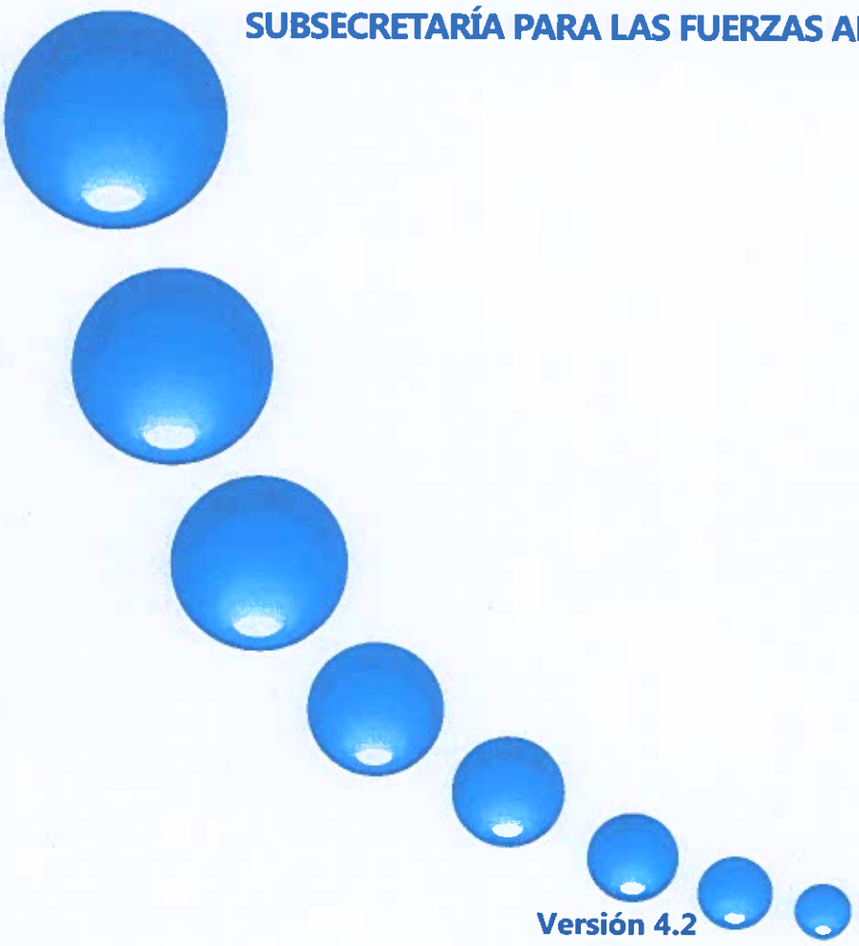
Subsecretaría para las Fuerzas Armadas

Gobierno de Chile

SSFFAA SSI

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

SUBSECRETARÍA PARA LAS FUERZAS ARMADAS



Versión 4.2
Diciembre 2018

ÍNDICE

I. DECLARACIÓN INSTITUCIONAL

La Subsecretaría para las Fuerzas Armadas es el órgano de colaboración del Ministro de Defensa Nacional en la formulación de políticas y la gestión de los asuntos y procesos administrativos que el Ministerio de Defensa Nacional, instituciones dependientes y relacionadas y las Fuerzas Armadas requieran para el desarrollo de la fuerza y el cumplimiento de sus funciones.

La Subsecretaría para las Fuerzas Armadas tiene como objetivos:

1. Gestionar los beneficios previsionales del sector pasivo de las Fuerzas Armadas y organismos dependientes, así como de sus familiares, generando oportuna y eficazmente los actos administrativos que conceden o regulan los beneficios previsionales y de seguridad social afectos al régimen previsional de las Fuerzas Armadas.

2. Gestionar y adoptar las acciones necesarias para el desarrollo de la carrera funcionaria de las Fuerzas Armadas y organismos dependientes, generando oportuna y eficazmente los actos administrativos que la formalizan.

3. Administrar el borde costero litoral y lacustre de la República a través del otorgamiento de Concesiones Marítimas y Acuícolas, de la zonificación y de la formulación de políticas en los espacios de competencia del Ministerio de Defensa Nacional.

II. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Subsecretaría para las Fuerzas Armadas reconoce la importancia de identificar y proteger sus activos de información, evitando la modificación, divulgación o destrucción no autorizada, estableciendo su compromiso con la Seguridad de la Información a través de la definición de la Política General de Seguridad de la Información e implementando un Sistema de Gestión de Seguridad de la Información (SGSI), con el objeto de la preservación de la confidencialidad, integridad y disponibilidad de sus activos de información.

III. OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Política General de Seguridad de la Información tiene los siguientes objetivos:

Objetivo General

El objetivo principal de la seguridad de la información es mantener un ambiente razonablemente seguro, alineado con los objetivos estratégicos de la Subsecretaria

para las Fuerzas Armadas, y que permita proteger los activos de información, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información y el aseguramiento de la continuidad del servicio.

Objetivos Específicos

1. Especificar las medidas esenciales de seguridad que el Servicio debe adoptar, para resguardarse apropiadamente contra amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información, ocasionando alguna de las siguientes consecuencias:

   - Pérdida o mal uso de los activos de información.
   - Pérdida de la imagen institucional
   - Pérdida de la información sensible

2. Proponer controles objetivos, eficientes y alcanzables por la Subsecretaría para las Fuerzas Armadas, tomando como base, los controles indicados en el NCh-ISO 27001:2013.

3. Promover, sociabilizar y fortalecer en la Subsecretaría para las Fuerzas Armadas, acciones proactivas que permitan implementar comportamientos asociados al resguardo de los activos de información, a través de actividades de difusión.

4. Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.

5. Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la alta dirección y auditorías internas planificadas a intervalos regulares.

6. Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información.

IV. ALCANCE DE APLICACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El alcance de aplicación de la política relativo al Sistema de Gestión de Seguridad de la Información (SGSI), abarca a toda la institución, a todo el personal de cualquier calidad jurídica (planta, contrata, honorario, personal en comisión de servicio), divisiones, departamentos, comités u otras estructuras funcionales, que presten servicios en la Subsecretaría para las Fuerzas Armadas, en lo referido a los procesos, procedimientos, instrucciones, programas y planes a desarrollar por la institución, y que estén relacionados con la seguridad de la información.

V. MARCO GENERAL PARA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El marco general proporciona las bases sobre la cual, la institución construye y determina el alcance y naturaleza de la participación de la política general de seguridad de la información, relacionada con las leyes y normativas chilenas, entre las cuales se cuentan: la protección de datos personales, propiedad intelectual, delitos informáticos, uso de herramientas informáticas y computacionales y, cualquier otra que norme a esta institución en el futuro. Además, todos los activos de información de acuerdo a su naturaleza, indicada en la Ley N° 20.424.

La presente política cubre toda la información clasificada como: impresa, almacenada física y electrónicamente, gestionada por correo o usando medios electrónicos, medios audiovisuales, registros de audio y en general por cualquier otro medio.

La política general de seguridad de la información, adopta su base de contenidos, a partir del estándar NCh-ISO 27.001:2013 y los requisitos legales, normativos y contractuales relativos a la seguridad de la información que sean aplicables a la institución, como las Normas Técnicas para los órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos, establecida por el Ministerio Secretaría General de la Presidencia, así como toda la información que refiere al marco general de la seguridad de la información, considerado para el Sistema de Gestión de Seguridad de la Información, el cual se basa en leyes y decretos:

Ley N°20.285/2008	Ley sobre acceso a la información pública
Ley N°20.212/2007	Ley Modifica las leyes N° 19.553, N° 19.882, y otros cuerpos legales, con el objeto de incentivar el desempeño de los funcionarios públicos.
Ley N°17.336/2004	Ley sobre propiedad intelectual
Ley N°19.927/2004	Ley modifica códigos penales en materia de delitos sobre pornografía infantil
Ley N°19.880/2003	Ley que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado
Ley N°19.799/2002	Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma
Ley N°19.628/1999	Ley sobre protección de la vida privada
Ley 19.812/2002	Ley sobre protección de la vida privada y modifica Ley 19.628
Ley N°19.553/1998	Ley Concede asignación de modernización y otros beneficios que indica
Ley N°19.223/1993	Ley sobre figuras penales relativas a la informática
Decreto N°475/ 2012	Reglamento Ley 19.553 para la aplicación del

	incremento por Desempeño institucional del artículo 6° de la Ley y sus modificaciones
Decreto N°14/2014	Modifica Decreto N° 181, de 2002, que aprueba reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica
Instructivo Presidencial N° 05/2001	Define el concepto de Gobierno Electrónico. Contiene la mayor parte de las instrucciones referidas al desarrollo de Gobierno Electrónico en Chile.
Instructivo Presidencial N° 06/ 2004	Imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la administración del Estado, para dotar así de un mayor grado de seguridad a las actuaciones gubernamentales que tienen lugar por medio de documentos electrónicos y dar un mayor grado de certeza respecto de las personas que suscriben tales documentos.
Instrucción General N°2/2009	Designación de Enlaces con el Consejo para la Transparencia.
Instrucción General N°3/ 2009	Índice de Actos o Documentos calificados como secretos o reservados
Instructivo Presidencial N°08/2006	Imparte instrucciones sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado
Instructivo Presidencial N°4/2003	Imparte instrucciones sobre aplicación de la Ley de Bases de Procedimientos Administrativos
Orden Ministerial N°1 y N°2/2018	Directiva de Ciberseguridad para el Ministerio de Defensa Nacional y actualización de Directiva.
Instructivo Presidencial N°8/2018	Imparte instrucciones sobre ciberseguridad.

El tratamiento de la seguridad de la información de la Subsecretaría para las Fuerzas Armadas, estará definida sobre los acuerdos estipulados en el marco de la seguridad de la información propuesto por el gobierno de Chile.

La presente Política de Seguridad de la Información contiene el conjunto de normas o buenas prácticas, aplicadas para toda la Subsecretaría para las Fuerzas Armadas., la cual tiene por objetivo, disminuir el riesgo para la ejecución de las actividades y las tareas definidas en el plan de trabajo del Sistema de Gestión de Seguridad de la Información, garantizando así, el correcto proceso de implementación en términos de periodicidad y sistematización.

Manejo de los activos de Información

Para garantizar un adecuado manejo de la información, esta Subsecretaría cuenta con metodologías de trabajo establecidas, las que definen claramente cómo se deben "clasificar los activos de la información", que circulan en la institución, considerando para esto lo siguiente:

Clasificación de los activos de información

- Los propietarios/as de los activos de información, que tengan éstos bajo su responsabilidad, la deben clasificar como "Confidencial", "Uso Interno" o "Público" de acuerdo a la importancia respecto de la seguridad del activo para la Institución.

- Todo activo de información que no haya sido clasificado debe considerarse como de "Uso Interno", de manera que reciba los niveles de protección acordes a esta clasificación.

- El encargado/a de Seguridad de la información debe preocuparse de que los activos reciban la clasificación apropiada, de manera que las medidas de protección que se apliquen, correspondan a las necesidades reales de la Subsecretaría para las Fuerzas Armadas.

- Por cada uno de los niveles de clasificación establecidos, se deben definir medidas de protección específicas, las que serán aplicadas por todo el personal.

Uso de Activos de Información

- Todo uso de activos de información debe ser para propósitos de esta Subsecretaría, de acuerdo a las políticas, estándares y procedimientos que se definan, considerando criterios de buen uso.

- La Subsecretaría para las Fuerzas Armadas no permite el uso de los activos de información institucionales para fines personales.

- Los usuarios/as de activos de información:

  – No deben divulgar información de la Subsecretaría ni de sus usuarios/as externos/as, clasificada como "Confidencial" o de "Uso Interno", salvo expresa autorización del Propietario/a de la Información, quién deberá hacerse responsable de esta divulgación. Está prohibido que los usuarios/as extraigan información fuera de las dependencias de la organización si no han sido específicamente autorizados.

- Deben solicitar autorización por escrito al Propietario/a de la Información, cuando necesiten proporcionar información "Confidencial" o de "Uso Interno" a terceros. La entrega de esta información se realizará suscribiendo acuerdos de confidencialidad con el tercero y aplicando los controles específicos que se definan, y en los casos que la ley lo determine.

- Deben cumplir con todos los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deberán mantenerse alineadas con las leyes vigentes. Deben proteger sus elementos de control de acceso, como contraseñas, dispositivos y otros, ya que son individuales, intransferibles y de responsabilidad única de cada usuario/a (planta, contrata, honorario, personal en comisión de servicio).

- Deben reportar de acuerdo al procedimiento establecido, cualquier incidente que ponga en riesgo la seguridad de la información; para que se tomen las medidas necesarias.

VI. ROLES Y RESPONSABILIDADES

Se establecen responsabilidades en materias de aprobación, control, actualización, difusión, cumplimiento, capacitación y actualización de la presente política, las que estarán distribuidas de acuerdo con la estructura organizacional vigente (Ley N°20.424, Estatuto Orgánico del Ministerio de Defensa Nacional) y por la estructura interna del personal adoptada por la Institución.

Los roles y responsabilidades son:

Subsecretario(a) para las Fuerzas Armadas

- Establecer los lineamientos estratégicos de la Seguridad de la Información.
- Aprobar la Política General de Seguridad de la Información de la Subsecretaría para las Fuerzas Armadas.
- La promoción activa de una cultura de seguridad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.

Comité de Seguridad de la Información:

Será responsabilidad del Comité de Seguridad de la Información, la supervisión e implementación de los procedimientos y estándares tendientes a mejorar los procesos que intervienen en la entrega de productos y servicios, garantizando el desarrollo del Sistema de Seguridad de la Información. Para ello se debe contar con un equipo multidisciplinario, formado por profesionales y técnicos de todas las áreas

relevantes de esta Subsecretaría y se establecerán las responsabilidades y especializaciones para cada dominio de la NCh-ISO 27001:2013.

- Será responsable de supervisar la implementación de procedimientos y estándares que se desprendan de las políticas de seguridad de la información.
- Propondrá estrategias y soluciones específicas para la implantación de los controles necesarios velar por el fiel cumplimiento de la política.
- Concientizar a los usuarios sobre la aplicación de la política.
- Revisar anualmente la política, difundir la política a través de los medios disponibles en la Institución.
- Arbitrar conflictos en materia de seguridad de la información.

Encargado(a) de Seguridad de la Información:

Es nombrado/a por el/la Jefe/a del Servicio, tendrá la calidad de asesor/a directo de la autoridad en temas de seguridad de la información.

Sus funciones son:

- Presidir y organizar las actividades del Comité de Seguridad de la Información.
- Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la institución, el control de su implementación y velar por su correcta aplicación.
- Coordinará la respuesta a incidentes que afecten a los activos de información.
- Establecerá puntos de enlace con los encargados de seguridad de otras entidades públicas, para la cooperación y transferencia de conocimientos.

Jefes(as) de División:

Alinearse con la política general de seguridad de la información. Impondrán el liderazgo y el compromiso de todo el nivel directivo en la intervención de los procesos a mejorar, relacionados con seguridad de la información.

Jefes(as) de Departamento:

Controlar la correcta aplicación de la política del personal a su cargo, promover el uso de la política en materias de seguridad.

Usuarios(as):

Regir su actuar de acuerdo con la política, desarrollar sus actividades en el uso de sistemas de información y tratamiento de la información que maneje o conozca.

VII. DEFINICIONES

Para resguardar el correcto y adecuado uso de la información en todos los ámbitos de tratamiento, la institución contempla entre las principales definiciones:

Activo de información:
Es todo lo que tiene valor para la organización.

Confidencialidad:
Es la propiedad de la información que impide la divulgación de información a individuos, entidades o procesos no autorizados.

Integridad:
Es la propiedad de la información que busca mantener los datos libres de modificaciones no autorizadas.

Disponibilidad:
Es la propiedad de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Seguridad de la Información
Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, buscando mantener la confidencialidad, disponibilidad e integridad de los activos de información.

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 Armas, 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. 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:

- Guía Metodológica 2018 Red de Expertos
- NCh-ISO 27001:2013
- Instructivo de Elaboración de Documentos

X. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

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

XI. 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 General de Seguridad de la Información, 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 en la vulneración de los principios de la probidad administrativa, si la hubiera, de acuerdo a los establecido por Decreto con Fuerza de Ley N° 29, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo, Artículo 119 y siguiente.

XII. APROBACIÓN

Elaborado por

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

Revisado por

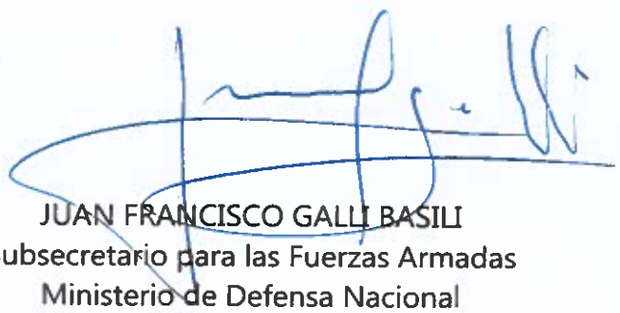
Juan Pablo Silva Ross
Jefe Departamento Tecnologías
de la Información y Comunicaciones
Subsecretaría para las Fuerzas Armadas

Visado por

JUAN IBACACHE IBACACHE
Jefe División Administrativa
Subsecretaría para las Fuerzas Armadas

JUAN IBACACHE IBACACHE
Jefe División Administrativa
SUBSECRETARIA PARA LAS FUERZAS ARMADAS

Aprobada por



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

XIII. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS DEL DOCUMENTO				
N° versión	Fecha	Motivo modificación	Páginas elaboradas y/o modificadas	Autor
1.0	03.12.2012	Elaboración inicial	Todas	Comité de Seguridad de la Información
2.0	14.06.2013	Aplicación de formato, ámbitos, definiciones, disposiciones de la política	Todas	Comité de Seguridad de la Información
3.0	03.10.2016	Revisión completa de la política	Todas	Igor Carrasco N.
4.0	14.09.2017	Aplicación de formato, cambio en los objetivos, revisión roles y responsabilidades, revisión de difusión de la política	Todas	Mauricio Arancibia P.
4.1	15.09.2017	Cambio en acciones especiales de seguridad, difusión de la política, definiciones	Pág 6,8,9	Juan Pablo Silva R.
4.2	10.12.2018	Cambio de formato, cambio en objetivos, revisión de difusión y periodicidad de revisión y evaluación	Todas	Mauricio Arancibia P.