

RESOLUCIÓN EXENTA N° 2130

Valparaíso, 06 MAYO 2019

VISTOS:

Lo dispuesto en el Decreto Supremo N° 83/03.06.04 del Ministerio Secretaría General de la Presidencia, que aprueba la norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad de los documentos electrónicos; la Norma Chilena ISO 27001/2013; los artículos 61 y siguientes de la Ley N° 18.834, sobre Estatuto Administrativo, y

CONSIDERANDO:

Que, mediante la Resolución Exenta N° 2.782, de 22.06.2018, el Director Nacional de Aduanas estableció la exigencia de implementar en el Servicio Nacional de Aduanas, el Sistema de Gestión de Seguridad de la Información, por lo que sancionó el texto, incorporándolo en la Política General de Seguridad.

Que, dicha política reconoce a la información como un bien valioso y fundamental para la institución, que debe ser administrado con igual atención que el resto de los activos del Servicio.

Que, en el marco del Programa de Mejoramiento de la Gestión e Implementación del Sistema de Seguridad de la Información del Servicio, se hace necesario introducir las modificaciones a las políticas, procedimientos y documentos, con el fin de adecuarlas a la nueva versión de la norma NCH/ISO27001:2013.

TENIENDO PRESENTE:

Lo dispuesto en la Resolución N° 1.600/30.10.08, de la Contraloría General de la República, sobre exención del trámite de toma razón, y las facultades que me confiere el artículo 4, número 15 del decreto con fuerza de ley N°329/79 del Ministerio de Hacienda, Ley Orgánica del Servicio Nacional de Aduanas, dicto la siguiente:

RESOLUCIÓN:

1.-MODIFÍCASE la Política General de Seguridad de la Información, la cual fue aprobada por Resolución Exenta N°5.973, de 03.10.2016, del Director Nacional.

La política modificada se encuentra contenida en el documento que se adjunta a esta resolución, la que se entiende forma parte de la misma.

2.- Los funcionarios del Servicio Nacional de Aduanas, deberán dar cumplimiento estricto a la Política General, y su infracción dará lugar a las responsabilidades que procedan, acorde al Estatuto Administrativo.





3.- Extiéndase la obligación de cumplir con la referida política -que por este acto se aprueba- a todo el personal contratado en calidad de honorarios, y a los terceros que se relacionen contractualmente con el Servicio, quienes serán responsables del cuidado de los activos de información del Servicio Nacional de Aduanas.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE EN LA INTRANET DEL SERVICIO NACIONAL DE ADUANAS.



[Handwritten signature in blue ink]
JOSÉ IGNACIO PALMA SOTOMAYOR
DIRECTOR NACIONAL DE ADUANAS



[Handwritten initials]
PIB/PDS/MTT/mtt

Distribución

Subdirecciones y Departamentos DNA

Correlativo N° **23378**



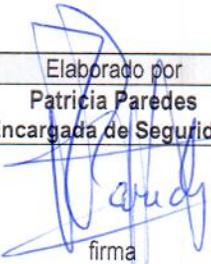
	Política General de Seguridad de la Información	
	PL-SNA-SSI-05.01.01	
Fecha emisión: 30/07/2016	Versión: 5	Fecha Revisión: 11/04/2019

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Sistema de Seguridad de la Información SNA

Código: PL-SNA-SSI-05.01.01

Versión: V5

Elaborado por Patricia Paredes Encargada de Seguridad	Revisado por Comité de Seguridad de la Información	Aprobado por Jose Ignacio Palma Director Nacional
 firma	Revisado en Acta de Aprobación CSI 11-04-2019	 firma

	Política General de Seguridad de la Información	
	PL-SNA-SSI-05.01.01	
Fecha emisión: 30/07/2016	Versión: 5	Fecha Revisión: 11/04/2019

Tabla de Contenidos

1.	DECLARACIÓN INSTITUCIONAL	3
2.	OBJETIVO DE LA POLÍTICA	3
3.	ALCANCE O ÁMBITO DE APLICACIÓN	3
4.	MARCO REGULATORIO	4
5.	GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS	5
6.	ROLES Y RESPONSABILIDADES	5
7.	MATERIAS QUE TRATA EL DOCUMENTO	5
8.	LINEAMIENTOS DE LA POLÍTICA	5
9.	PERÍODO DE VIGENCIA Y REVISIÓN	7
10.	MECANISMO DE DIFUSIÓN	7
11.	EVALUACIÓN DE CUMPLIMIENTO	7
12.	HISTORIAL DE MODIFICACIONES (CONTROL DE CAMBIOS)	8

	Política General de Seguridad de la Información	
	PL-SNA-SSI-05.01.01	
Fecha emisión: 30/07/2016	Versión: 5	Fecha Revisión: 11/04/2019

1. DECLARACIÓN INSTITUCIONAL

La presente Política General de Seguridad de la Información del Servicio Nacional de Aduanas, define los objetivos, alcances y principios esenciales para la administración, custodia y el uso de los activos de información, velando por su disponibilidad, confidencialidad e integridad, acorde a la normativa legal y reglamentaria vigente.

Constituyen activos de información, todo aquello que tenga valor y que contenga información relevante para el Servicio Nacional de Aduanas, cualquiera sea su soporte, los equipos y sistemas que los almacenan o procesen y las personas que los administran o utilicen.

2. OBJETIVO DE LA POLÍTICA

La Política General de Seguridad de la Información del Servicio Nacional de Aduanas, tiene los siguientes objetivos:

- Resguardar los activos de información del Servicio Nacional de Aduanas frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información, considerándolos resultados de la evaluación y tratamiento de los riesgos.
- Implementar medidas especiales de seguridad, teniendo como base esta Política General.

3. ALCANCE O ÁMBITO DE APLICACIÓN

- Esta política está dirigida a todo funcionario planta o contrata del Servicio Nacional de Aduanas, asesores, personal a honorarios o terceros, que tenga acceso a información de la Institución.
- En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta Política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Dominios y Controles de Seguridad relacionados	
A.5	Dominio: Política de Seguridad de la Información
A.05.01.01	Política para la seguridad de la información
A.05.01.02	Revisión de las políticas de seguridad de la información

- En cuanto al ámbito institucional de aplicación de esta Política, responde a los siguientes objetivos y productos estratégicos del formulario A1, relacionados con los referidos procesos críticos, lo que se corresponde con el alcance declarado del Sistema de Seguridad de la Información del Servicio:

Objetivo, Producto estratégico y Proceso crítico en ámbito de aplicación		
Objetivo Estratégico	Producto Estratégico A1	Proceso crítico protegido
Objetivo Estratégico. (1) y (3)	(1) Fiscalización de las Operaciones de Comercio Exterior.	Fiscalización.
Objetivo Estratégico. (1) ,(2) y (3)	(2) Provisión de Operaciones de Comercio Exterior.	Despacho de Mercancías.
Objetivo Estratégico. (1) ,(2) y (3)	(3) Estadísticas de Comercio Exterior.	Gestión de Información.
Objetivos Estratégicos referenciados:		
(1) Desarrollar y aplicar estrategias diferenciadas para una fiscalización ágil e inteligente, según el nivel de cumplimiento de los operadores y los riesgos prioritarios del país.		
(2) Fomentar el cumplimiento voluntario, a través de la optimización de procesos y normativa basada en estándares internacionales, y el diseño e implementación de programas que facilitan las operaciones		

	Política General de Seguridad de la Información	
	PL-SNA-SSI-05.01.01	
Fecha emisión: 30/07/2016	Versión: 5	Fecha Revisión: 11/04/2019

aduaneras.

(3) Establecer estrategias de explotación, desarrollo y mantención de plataformas de tecnologías de la información que soporte los procesos, para garantizar una gestión integrada y eficiente, y con ello, asegurar la prestación de un servicio oportuno y de calidad a nuestros usuarios.

4. MARCO REGULATORIO

- El marco jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
 - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
 - Decreto Supremo N° 1.299/2004, Establece nuevas normas que regulan la Red de Conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas.
 - Decreto Supremo N° 5.996/1999, Crea Red Interna (INTRANET) del Estado y entrega su implementación, puesta en marcha, administración, coordinación y supervisión al Ministerio del Interior, Trámite extraordinario de urgencia.
 - Decreto Supremo N° 1/2015, Aprueba norma técnica sobre sistemas y sitios web de los Órganos de la Administración del Estado.
 - Decreto Supremo N° 83/2005, Aprueba norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad de los documentos electrónicos.
 - Decreto Supremo N° 93/2006, 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° 14/2014, Modifica el Decreto N° 181, de 2002, que aprueba el Reglamento de la Ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica.
 - Decreto Supremo N° 1/2015, Aprueba norma técnica sobre sistemas y sitios web de los Órganos de la Administración del Estado.
 - Leyes relacionadas
 - Ley N° 20.285/2008, Ley sobre acceso a la información pública.
 - Ley N° 17.336/2004, Ley sobre propiedad intelectual.
 - Ley N° 19.927/2004, Ley que modifica el Código Penal. El Código Procesal Penal y Código Penal, 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 N° 19.223/1993, Ley sobre figuras penales relativas a la informática.
 - Ley N° 19.628/1999 Ley sobre protección de la vida privada.
 - Ley N° 19.223/1993 Ley sobre figuras penales relativas a la informática.
 - Ley N° 20.478/2010 Ley sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones.
- Documento de Identificación de Legislación vigente y los requisitos contractuales(18.01.01)
- NCH-ISO 27001 vigente. Tecnología de la información – Sistemas de gestión de la seguridad de la información – Requisitos.
- Manual de Sistema de Gestión de la Seguridad de la Información.
- La Política Nacional de Ciberseguridad.

	Política General de Seguridad de la Información	
	PL-SNA-SSI-05.01.01	
Fecha emisión: 30/07/2016	Versión: 5	Fecha Revisión: 11/04/2019

5. GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS

Las definiciones necesarias para la comprensión del contenido de este procedimiento y las restantes definiciones generales; y el glosario de términos y acrónimos utilizados en los documentos del Sistema de Seguridad de la Información del Servicio, se encuentran integrados en el Manual de Sistema de Gestión de la Seguridad de la Información, en la sección "Glosario Términos, definiciones y siglas del SSI", publicado en la intranet institucional, en el banner Sistema de Seguridad de la Información.

6. ROLES Y RESPONSABILIDADES

El Servicio Nacional de Aduanas mantendrá una adecuada organización relacionada con la seguridad de la información, la cual contendrá a lo menos un Comité de Seguridad de la Información y un Encargado de Seguridad de la Información.

- El Comité de Seguridad de la Información deberá proponer las medidas de seguridad destinadas a proteger y preservar los activos de información de la institución y velar por el cumplimiento de todo lo establecido en los documentos del SGSI.
- El Encargado de Seguridad de la Información deberá, entre otras materias, coordinar la implantación y efectiva aplicación de las medidas de seguridad que se definan.

Además esta Política General es aplicable y extensiva a todo el personal del Servicio, independiente de su modalidad de contratación; y a terceros, naturales o jurídicos, que presten servicios permanente o temporalmente en el Servicio Nacional de Aduanas.

Consecuente con lo anterior, los terceros deberán conocer y acatar la presente Política y las que de ésta se desprendan, lo que quedará expresamente consignado en los respectivos contratos o acuerdos de servicio.

El detalle de los roles y responsabilidades del Sistema de Gestión de Seguridad de la Información, se encuentran descritas en la Política de Seguridad de Roles y Responsabilidades (A06.01.01), la que se encuentra publicada en la intranet del Servicio Nacional de Aduanas.

7. MATERIAS QUE TRATA EL DOCUMENTO

Establecimiento del enfoque de la Política en línea con los objetivos institucionales del Servicio Nacional de Aduanas y el apoyo y compromiso con la seguridad de la información.

8. LINEAMIENTOS DE LA POLÍTICA

El Servicio Nacional de Aduanas, declara que es de primordial importancia la seguridad de la información en su quehacer diario, por lo que se compromete a gestionar la Seguridad de la Información como un proceso continuo, a través de la implementación de un Sistema de Gestión basado en la norma Nch-27001, de acuerdo a la legislación vigente, y bajo los siguientes lineamientos:

- a) Se reconoce la información como activo, valioso y fundamental para la institución, que debe ser administrado con igual atención que el resto de los activos de la institución.

	Política General de Seguridad de la Información	
	PL-SNA-SSI-05.01.01	
Fecha emisión: 30/07/2016	Versión: 5	Fecha Revisión: 11/04/2019

- b) Se define como Seguridad de la Información, toda acción que busque proteger la integridad, confidencialidad y disponibilidad de los activos de información institucionales.
- c) Se reconoce a la Seguridad de la Información como un atributo necesario de los servicios ofrecidos por la institución.
- d) Los activos de información deben ser protegidos adecuadamente.
- e) El Servicio Nacional de Aduanas incorpora en sus políticas de seguridad de información los controles y resguardos necesarios para cumplir con las regulaciones legales, relacionadas con la reserva y privacidad de la información.
- f) El Servicio Nacional de Aduanas reconoce el compromiso, de toda la organización, de cautelar y velar por la confidencialidad y reserva de la información, que las instituciones, los agentes de comercio exterior, las empresas, las personas naturales y sus funcionarios, le han proporcionado u obtenido en el ejercicio de sus funciones; y también, a suministrar la disponibilidad de acceso a esta información.
- g) La Seguridad de la Información asociado a su manejo, es responsabilidad de todos los funcionarios, independiente del cargo o funciones que desempeñen; y de terceros.
- h) La información sujeta a confidencialidad o reserva, de acuerdo al marco legal vigente, no debe quedar disponible a personas o entidades externas, salvo en las situaciones y formas expresamente establecidas en las normas vigentes y con controles que garanticen su protección.
- i) Las normas y políticas sobre Seguridad de la Información, serán debidamente controladas y auditadas en su cumplimiento por las unidades correspondientes de la institución.
- j) El incumplimiento de las obligaciones emanadas de esta Política General, de las políticas específicas, procedimientos u otros documentos de Seguridad de la Información específicos que emanan de esta, serán sancionadas bajo los términos establecidos en el Estatuto Administrativo. En el caso de infracción grave realizada por "terceros", se podrá poner término a su contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades penales y legales que se deriven de tales infracciones.
- k) En los casos donde exista una necesidad justificable de realizar acciones excepcionales, que estén en conflicto con las medidas establecidas en la política de Seguridad del Servicio Nacional de Aduanas, deberán ser evaluadas y aprobadas por el Comité de Seguridad.
- l) El Servicio asegura que se desarrollarán los procesos, a través de una correcta segregación de funciones que permita garantizar la ejecución, revisión, autorización y seguimiento a diferentes niveles.
- m) La Política General de Seguridad de la Información, así como las que se desprendan de ella, se difundirán a través de la Intranet del Servicio Nacional, algunas de ellas también serán publicadas en la página web, sin perjuicio de su sensibilización al interior de la Institución, para lo cual podrán realizarse charlas, cursos, talleres y/o publicaciones u otras actividades.

	Política General de Seguridad de la Información	
	PL-SNA-SSI-05.01.01	
Fecha emisión: 30/07/2016	Versión: 5	Fecha Revisión: 11/04/2019

De esta Política General, se desprenderán las restantes Políticas de Seguridad de la Información, que constituyen, definen y complementan dicha Política General de la Institución en materias específicas; precisando el rol que deben asumir los funcionarios y terceros para el resguardo de la información y de sus recursos asociados. Las Políticas específicas son las siguientes:

- Política de roles y responsabilidades de la seguridad de la información
- Política de dispositivos móviles
- Política de trabajo remoto
- Política de seguridad en gestión de personas
- Política de seguridad de sanciones
- Política de control de acceso de los activos de la información
- Política de acceso a las redes y a los servicios de la red
- Política de controles de criptográficos
- Política de gestión de claves criptográficas
- Política de seguridad de escritorio y pantallas limpias
- Política de gestión de cambios
- Política de respaldo de la información
- Política de registro de evento
- Política de restricciones en la instalación de software
- Política de transferencia de información
- Política de desarrollo seguro
- Política de relación con proveedores
- Política de gestión de incidentes de seguridad de la información
- Política de planificación de la continuidad de la seguridad de la información
- Política de privacidad y protección de datos personales

9. PERÍODO DE VIGENCIA Y REVISIÓN

Esta política tiene una vigencia de tres años, sin embargo, se efectuará una revisión del contenido de este documento anualmente por el Comité de Seguridad de la Información (CSI) del Servicio; o cuando deban atenderse necesidades de cambios significativos, para garantizar su idoneidad, adecuación y efectividad; o, cuando sea presentado como requerimiento expreso de cualquiera de sus miembros.

10. MECANISMO DE DIFUSIÓN

Esta política quedará disponible en banner Sistema de Seguridad de la Información de la Intranet del Servicio y sitio web del Servicio Nacional de Aduanas.

11. EVALUACIÓN DE CUMPLIMIENTO

La evaluación de la aplicación de esta Política, se realizará al menos cada tres años. Su mecanismo de evaluación quedará establecido en el Manual del Sistema de Gestión de la Seguridad de la Información.

	Política General de Seguridad de la Información	
	PL-SNA-SSI-05.01.01	
Fecha emisión: 30/07/2016	Versión: 5	Fecha Revisión: 11/04/2019

12. HISTORIAL DE MODIFICACIONES (CONTROL DE CAMBIOS)

Revisión Nº	Párrafo	Cambio	Fecha	Responsable
V0		Creación del Documento	30/07/2016	Estudios
V1	En Alcance	Se agregó el sgte. Párrafo: "La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización basándose en metodologías de mejoramiento continuo."	01/09/2016	Estudios
V1	Punto 7	Se elimina Texto " y de los bienes"	01/09/2016	Estudios
V1	Punto 9	Se elimina Texto:", al menos cada 3 años. La infracción a dichas normas y políticas estará sujeta a posible sanciones"	01/09/2016	Estudios
V1	Se agrega punto	Se agrega medidas a tomar ante incumplimientos	01/09/2016	Estudios
V1	Punto 11	Se modifica medios de difusión	01/09/2016	Estudios
V2	Todo el documento	Cambio de formato y ajustes de redacción	11/08/2017	Estudios
V3	En lineamientos	Se agregó el manejo de excepciones a la política	11/12/2017	Estudios
V3	En general	Se incluyen referencias al manual de seguridad	11/12/2017	Estudios
V4	En lineamientos	Se mejora redacción	01/06/2018	Estudios
V4	En difusión	Se modifican algunos medios de difusión	01/06/2018	Estudios
V4	En lineamientos	Se agregan políticas específicas	01/06/2018	Estudios
V5	En alcance	Se modifica el nombre de un producto estratégico	11/04/2019	Estudios