Superintendencia del Medio Ambiente
Gobierno de Chile

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Aprobado por:	Versión
Departamento de Gestión de la Información	Comité de Seguridad de la Información	Noviembre 2017

Control de versiones:

N° Revisión	Fecha Aprobación	Motivo de la revisión	Autor
01	Mayo 2011	Elaboración inicial	Pablo Quintana – Encargado Sistemas TI
02	Enero 2012	Corrección de contenido	Pablo Quintana – Encargado Sistemas TI
03	Mayo 2013	Corrección de contenido	Marco Bassaletti – Encargado Unidad TI
04	Octubre 2014	Corrección de contenido	Marco Bassaletti – Encargado Unidad TI
05	Noviembre 2017	Ajuste de formatos de acuerdo a lo instruido por la Red de Expertos del PMG-SSI 2017	Sebastián Elgueta – Jefe de Departamento de Gestión de la Información

1. Declaración Institucional

La Superintendencia del Medio Ambiente, en adelante, SMA, promueve y apoya activamente las acciones que permitan mantener un alto nivel de seguridad de la información, definida ésta como: "la preservación de la confidencialidad, integridad y disponibilidad de los activos de información, necesarios para alcanzar los objetivos de la organización", dado que los activos de información poseen valor para la organización, por lo que deben ser protegidos adecuadamente a fin de que permitan cumplir la misión institucional.

Según lo expuesto, la SMA se compromete a desarrollar y ejecutar un plan de acción de mejora continua de manera de asegurar una adecuada gestión de la seguridad de la información en sus diferentes ámbitos de aplicación, según lo dispuesto en la Norma Chilena de Seguridad de la Información y otras normativas vigentes relacionadas como la Modernización del Estado, el Gobierno electrónico, la Transparencia y Acceso a la Información Pública, de Protección a la Vida Privada y de Datos Personales, Procedimientos Administrativos, entre otras.

La presente Política General de Seguridad de la Información, define las directrices, objetivos, alcances esenciales para la custodia y el uso de los activos de información y de los bienes asociados a su tratamiento, velando por su disponibilidad, confidencialidad e integridad, acorde a la normativa legal y reglamentaria vigente.

2. Importancia de la Política General de Seguridad de la Información

La importancia de la Política de Seguridad de la Información se expresa en los siguientes principios:

- Se reconoce la información como un activo, valioso y fundamental para la institución, que debe ser administrado con igual atención que el resto de los activos de la institución.
- Se define como Seguridad de la Información, toda acción que busque proteger la integridad, confidencialidad y disponibilidad de los activos de información institucionales.
- Se reconoce la seguridad de la información como un atributo necesario de los servicios ofrecidos por la institución.
- Los activos de información deben ser protegidos adecuadamente.
- La institución incorpora en sus políticas de seguridad de información los controles y resguardos necesarios para cumplir con la normativa relacionada con la reserva y privacidad de la información.
- La institución 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 proporcionar la disponibilidad de acceso a esta información.

- La seguridad de la información y de los bienes asociados a su manejo, es responsabilidad de todos los funcionarios y terceros independientemente del cargo o funciones que desempeñen.
- 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.

3. Objetivo de la Gestión de Seguridad de la Información

La gestión de seguridad de la información en la Superintendencia del Medio Ambiente tiene como principales objetivos:

- Proteger adecuadamente los activos de información institucionales.
- Implementación y propender al cumplimiento de las políticas generales y específicas, normas, procedimientos, prácticas y estándares referentes a la seguridad de la información.
- Clasificar la información según su grado de sensibilidad e implementar mecanismos de seguridad adecuados a dicha categoría
- Realizar una evaluación de riegos periódica, cuyos resultados ayudarán a orientar la implementación de controles para proteger la información afecta a dichos riesgos.
- Implementar técnicas para la gestión del riesgo utilizando como base la familia de la normativa NCh-ISO 27000.
- Impulsar el desarrollo, cumplimiento y mantenimiento de un Plan de Continuidad del Negocio, el cual debe entenderse como un proceso de carácter cíclico y continuo.
- Realizar difusión permanente de las Directrices de Seguridad de la Información, con el objeto de sensibilizar a todos los usuarios de la Superintendencia del Medio Ambiente, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes y otros, en el cumplimiento de las medidas de seguridad establecidas.
- Revisar, monitorear, auditar y mejorar continuamente las directrices de seguridad que garanticen el mantenimiento de los niveles de seguridad requeridos.

- Destinar los recursos necesarios para desarrollar todas las medidas de seguridad que se determinen, mantenimiento un adecuado balance entre costo y beneficio.
- Dar cumplimiento a la normativa vigente.

4. Alcance de la Política de Seguridad de la Información

La Política General de Seguridad de la Información se aplicará a todos los activos de información, independientemente de su soporte o almacenamiento, de los sistemas que lo procesen o de los métodos de transporte utilizados (base de datos, respaldos magnéticos, información impresa, internet y otros) y las personas que tengan acceso, manipulen o utilicen dichos activos en el cumplimiento de sus labores.

Los ámbitos de control, o dominios de seguridad de la información, especificados en la NCh-ISO 27001.Of2013 y NCh-ISO 27002.Of2013 a los que aplica la política, son los siguientes:

A.05.01.01 – Conjunto de políticas para la seguridad de la información.
A.05.01.02 – Revisión de las políticas para la seguridad de la información.

5. Roles y Responsabilidades

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.

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, y adicionalmente aprobar los procedimientos operativos que se generen dentro de la implementación del Sistema de Seguridad de la Información.

Cada funcionario y terceros relacionados al Servicio, deberán acceder exclusivamente a la información que sea necesaria para cumplir sus labores y tendrán la obligación de notificar cualquier actividad o situación que contravenga estos lineamientos. Se entenderá por "terceros" a todos aquellos que, no siendo funcionarios de planta o a contrata, tengan acceso a activos de información del Servicio, incluidos los empleados y representantes de las personas naturales o jurídicas con quienes el Servicio mantenga algún tipo de relación.

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.

6. Medios de Difusión

La Política General de Seguridad de la Información, así como las políticas que se desprendan de ella, se difundirán a través de la intranet del Servicio, de su página web y boletín, según corresponda.

La responsabilidad de la difusión de la Política General de Seguridad será de responsabilidad del Encargado de Seguridad de la Información.

7. De la Revisión de esta Política

La Política General, las políticas específicas que de ella se desprendan y los procesos que las soporten, deberán ser revisados por lo menos una vez cada dos años o ante cualquier cambio significativo de tecnología, personal o evento que amerite su reevaluación para asegurar su continuidad, idoneidad, eficiencia y efectividad.

8. Evaluación del cumplimiento de la política

Las normas y políticas sobre Seguridad de la Información serán debidamente controladas y auditadas en su cumplimiento por las unidades correspondientes de la institución cada 2 años.

9. Sanciones

Las faltas incurridas en el cumplimiento de las obligaciones y deberes establecidos en la Política General de Seguridad de la Información y en las políticas específicas que la acompañen, por parte de los funcionarios, se considerarán como un incumplimiento de las obligaciones funcionarias contempladas en el artículo 61 del D.F.L. 29/2014 que fija el texto refundido, coordinado y sistematizado de la Ley 18.834, Estatuto Administrativo, y podrán dar origen a procesos administrativos disciplinarios, ya sea investigación sumaria o sumario administrativo.

Lo anterior, con independencia de las responsabilidades civiles o penales que pudiera acarrear alguna infracción de estas normas o sus consecuencias.

En cuanto al personal que preste servicios a honorarios, estará sujeto a cláusulas de confidencialidad y apego a estas disposiciones, las cuales formarán parte de su respectivo convenio de prestación de servicios. Su incumplimiento se considerará como incumplimiento del contrato pudiendo implicar el término anticipado e inmediato de éste, siéndoles, además, plenamente aplicables las responsabilidades civiles o penales que pudiera acarrear alguna infracción a estas normas o sus consecuencias.

Del mismo modo, se perseguirán las responsabilidades civiles o penales que pudieran acarrear alguna infracción a estas normas, o sus consecuencias, por parte de

proveedores u otros prestadores de servicios (contratistas y usuarios de terceros), respecto de los cuales deberán considerarse medidas de información y suscripción.

10. Principios de confidencialidad

Toda la información y documentación electrónica que genera, y procesa la SMA debe ser tratada desde el punto de vista de la confidencialidad, de acuerdo a la normativa de la Ley Nº 20.285 y el reglamento establecido DS Nº 13, de 2009, del Ministerio Secretaría General de la Presidencia, sobre el acceso a la información pública.

Además, deberá ser considerado lo establecido en la ley orgánica de la SMA, respecto de los registros públicos de sanciones y los expedientes de los procesos de fiscalización y sanción.

11. Glosario

Para los propósitos de esta Política, las siguientes palabras se entenderán en el sentido que a continuación se indica:

Activo: todo aquello que tenga valor para la organización. Para el ámbito de seguridad de la información, se puede clasificar en:
a) Activos de Información.
b) Activos de Software: Constituidos por las Aplicaciones de software, Software de sistemas y, Herramientas de desarrollo y utilidades.
e) Activos Físicos: Constituidos por el Equipamiento computacional, Equipamiento de comunicaciones, Medios móviles y otros equipamientos.
d) Servicios: Servicios de computación y comunicaciones. Utilidades generales (ej. electricidad, luz, aire acondicionado, etc.)
e) Personas: Constituidos por los usuarios, que utilizan la estructura tecnológica, el área de comunicaciones y que gestionan la información.
f) Intangibles: Constituidos por los activos referidos a la reputación e imagen de la institución.

Activo de información: Los Activos de Información corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta forma podemos distinguir 3 niveles básicos de activos de información:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- Los Equipos/Sistemas/infraestructura que soportan esta información.
- Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

Amenaza: Una causa potencial de un incidente no-deseado, el cual puede derivar en daño a un sistema u organización.

Control: Medios para manejar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas, o estructuras de la organización, que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos de información.

Política: Intención y dirección general expresada por la Jefatura del Servicio.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades, tales como autenticidad, responsabilidad con obligación de informar, no repudio y confiabilidad.

Soporte de procesamiento de la información: Todo sistema de procesamiento de la información, servicio o infraestructura, o las localizaciones físicas que los contienen.

Tecnología de la Información y de las Comunicaciones (TIC): Constituida por la agrupación de los elementos y las técnicas utilizadas en el tratamiento y la transmisión de la información, principalmente de informática, internet y telecomunicaciones.