POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

SERVICIO DE EVALUACIÓN AMBIENTAL

APROBACIÓN

La presente Política General de Seguridad de la Información, versión 8.0, ha sido aprobada por el Director Ejecutivo del Servicio de Evaluación Ambiental, y tiene vigencia a partir de la fecha de su firma electrónica.

FIRMA Y TIMBRE DIRECTOR EJECUTIVO

NOTA DE CONFIDENCIALIDAD

La información contenida en el presente documento es de propiedad y uso exclusivo del Servicio de Evaluación Ambiental, para los fines que determine y no podrá ser modificado ni utilizado en otra institución sin previa autorización del Comité de Seguridad de la Información de este Servicio.

Elaborado por	Revisado por	Aprobado por	Aprobado por
Fernando Jofré Alfonso Encargado de Seguridad de la Información	Iván Parra González Jefe Departamento Soporte Administrativo	Hernán Joglar Espinosa Jefe de División de Tecnologías y Gestión de la Información	Genoveva Razeto Cáceres Jefa de División Jurídica

HISTORIAL DE VERSIONES

Tabla de Identificación y Control de Cambios

Versión	Fecha	Sección	Resumen de modificaciones o motivos	Elaborado por	Revisado por
8.0	03/12/2021	1.3 2. 3. 4.3 4.4 5. 6. 11.	Se complementa el párrafo Se elimina mención a Objetivo General. 1. Se agrega la frase "la disponibilidad" al alcance. 2. Se referencia al documento de origen del producto estratégico. Se referencia a resolución de nombramiento Eliminado. Se referencia al documento MA-SGSI-01 Se menciona responsabilidad del Depto auditoría Eliminado.	Fernando Jofré Alfonso Encargado de Seguridad de la Información	Hernán Joglar Espinosa, Jefe División Tecnologías y Gestión de la Información Iván Parra G. Jefe Depto Soporte Administrativo
7.0	14/08/2019	Todas	1. Todos los capítulos. 2. Revisión y actualización. 3. Se actualizó el alcance y se simplifico, en tal sentido la especificación de los 14 dominios y sus 35 objetivos se desarrollarán en las políticas específicas por dominio. 4. Se actualizaron los objetivos del SGSI.	Rodrigo Cerda A.	Hernán Joglar Espinosa, Jefe División Tecnologías y Gestión de la Información Iván Parra G. Abogado de la División Jurídica
6.0	10/08/2018		1. Evaluación de la Política 2. Revisión de la Política 3. Actualización de la Política	Rodrigo Cerda A.	Iván Parra G. Abogado de la División Jurídica
5.0	15/09/2017	Todas	1. Evaluación de la Política 2. Revisión de la Política 3. Actualización de la Política	Ricardo Oliva S.	Rodrigo Cerda A. Encargado de Seguridad de la Información y Jaime Guarello M. Abogado de la División Jurídica
4.0	10/04/2015		1. Todos los capítulos. 2. Revisión y Actualización 3. Se mejoró y actualizó los puntos relacionados con el uso correos electrónicos y respaldo de Información 4. Se agregó las materias relacionadas con el uso de las herramientas colaborativas	Ricardo Oliva S.	Hernán Joglar Espinosa, Jefe División Tecnologías y Gestión de la Información Rodrigo Cerda A. Jefe Depto. de Infraestructura y Operaciones Javier Herrera, Abogado División Jurídica

Versión	Fecha	Sección	Resumen de modificaciones o motivos	Elaborado por	Revisado por
					Juan Moscoso Farías, Jefe División Jurídica
3.0	07/08/2013	Gestión y usabilidad de activos de información	1. Se agregaron los dominios de la ISO 27001 como nuevas secciones: 2. Política general de seguridad 3. Organización de la seguridad de la información 4. Gestión de activos 5. Seguridad de los recursos humanos 6. Seguridad física y del ambiente 7. Gestión de las comunicaciones y operaciones 8. Control de acceso 9. Adquisición, desarrollo y mantenimiento de los sistemas de información 10. Gestión de incidentes en la seguridad de la información 11. Política general de gestión de la continuidad del negocio 12. Política general de cumplimiento legal, estatutario y regulatorios 13. Se eliminó la sección GESTIÓN Y USABILIDAD DE ACTIVOS DE INFORMACIÓN. Se reorganizaron sus temas: i) Correo Electrónico ii) Cuentas de Usuario iii) Antivirus iv) Respaldo de Información v) Uso de Internet vi) Uso de Equipamiento Computacional 14. Se eliminó la sección CLASIFICACIÓN DE LA INFORMACIÓN; sus temas fueron agregados a los dominios de la ISO que los contienen. 15. Se mejoró el Glosario de Términos 16. Roles y Responsabilidad 17. Revisión de cumplimiento	Guiomar Leiva	Ricardo Oliva Encargado de Seguridad de la Información Rodrigo Cerda Jefe del Departamento de Infraestructura y Operaciones José Adolfo Moreno Jefe de la División Jurídica
2.0	29/08/2012	Todas	Se actualizó completamente la Política general de seguridad de la información en todos sus puntos.	Ricardo Oliva S.	- Rodrigo Cerda A. Encargado de Seguridad -Matías Montoya T. Jefe de la División Jurídica
1.0	25/07/2011	Todas	Elaboración	José Luis Sepúlveda	Carlos Pinilla M. Jefe de la División de Tecnologías y Gestión de la Información

INDICE DE CONTENIDO

1. DECLARACIÓN INSTITUCIONAL

Los riesgos sobre los activos de información en las organizaciones actuales son relevantes y están siempre presentes. Es por ello que el Servicio de Evaluación Ambiental se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo a través de un programa de implantación que se denominará "Sistema de Gestión de Seguridad de la Información (SGSI)", el cual está basado en la norma NCh-ISO 27001:2013, y en cumplimiento con lo establecido en el Decreto Supremo Nro. 83 del Ministerio Secretaria General de la Presidencia, de fecha 03 de junio de 2004, sobre la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, la Ley N° 20.285 sobre Acceso a la Información Pública, la Ley N° 19.628 sobre de Protección de la Vida Privada, la Ley N° 18.834 que aprueba Estatuto Administrativo y por último, considerando los lineamientos de la Red de Expertos del PMG de Seguridad de la Información, tendientes a homogenizar los criterios de seguridad en los Servicios Públicos.

La presente política de seguridad entrega las directrices respecto de la forma en que debe implementarse la seguridad de la Información de acuerdo a las normativas vigentes.

1.1. Definiciones claves de Seguridad de la Información

Se entenderá por **Activo de Información** todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución. En este sentido, podemos distinguir 3 tipos de activos:

- La Información propiamente tal, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, otros.)
- Los equipos, sistemas u otros medios que se consideren.
- Las personas que la utilizan.

1.2. Criterios de Seguridad

El Sistema de Gestión de Seguridad de la Información (SGSI) establecerá distintos controles tanto a nivel de gobierno corporativo como de gestión, con el objeto de garantizar que los activos de información cumplan con los siguientes atributos:

- **Confidencialidad**: Los activos de información se encuentran protegidos de personas/usuarios no autorizados.

- **Integridad**: Los activos de información se encuentran completos, actualizados y son veraces, sin modificaciones inapropiadas o corruptas.

- **Disponibilidad**: Los usuarios autorizados pueden acceder a los activos de información cuando requieran utilizarlos para desempeñar sus funciones.

1.3. Importancia para la Institución

Los activos de información que se generan como producto del quehacer institucional cobran real importancia para los procesos de negocios institucionales, pues estos aportan valor a los procesos y son considerados un bien para la Institución; en virtud de esto requieren ser protegidos de forma correcta ante cualquier amenaza, con el propósito de asegurar la continuidad de las operaciones y la eficiencia de la gestión del Servicio de Evaluación Ambiental (en adelante e indistintamente también, el "SEA", el "Servicio" o la " Institución").

En este sentido, implementar un Sistema de Gestión Seguridad de la información (SGSI) en el SEA, conlleva a garantizar el correcto manejo de los activos de información, de manera de gestionar sus riesgos asociados, generar mayores beneficios para los ciudadanos y evitar el uso indebido de los mismos. En este sentido, esta política general se presenta como una herramienta organizacional para interiorizar a cada uno de los miembros de este Servicio sobre la importancia y sensibilidad de la información generada al interior de la Institución, junto con dar a conocer y orientar el uso de los servicios que la soportan.

2. OBJETIVOS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

a) Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información crítica del SEA, con el objeto de asegurar continuidad operacional de sus productos estratégicos, a través de un sistema de gestión de seguridad de la información, en apoyo al cumplimiento de los objetivos de la institución y del servicio hacia los ciudadanos y beneficiarios.
b) Contar con una visión global sobre el estado de los activos de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación.
c) Diseñar y ejecutar planes de capacitación e inducción continua, los cuales fortalezcan los conocimientos y sensibilicen al personal de la Institución, en materias de seguridad de la información.

3. ALCANCE

Esta política debe ser aplicada y extensible a toda la dotación de la Institución y a las personas externas que presten servicios permanentes o temporales en ella, que involucren o no sistemas de información de la Institución, abarcando toda forma de tratamiento y almacenamiento de información, de acuerdo a las definiciones de tipo de activo de la información entregada en el punto 1.1 precedente.
En tal sentido, la presente política abarca los activos de información relevantes que forman parte del alcance de aplicación definido del SGSI, actuales o futuros, por tanto, la no inclusión explícita de alguno de ellos en el presente documento no constituye argumento para no protegerlos.

Como primer alcance de implementación del SGSI en el SEA para enfrentar el proceso de certificación en la normativa ISO/IEC 27001:2013, se define lo siguiente:

> "Mantener eficientemente la disponibilidad del Sistema de Evaluación de Impacto Ambiental Electrónico (e-SEIA)".

Este alcance constituye el proceso fundamental para garantizar la continuidad en la operación del producto estratégico[1] "Administrar el Sistema de Evaluación de Impacto Ambiental electrónico", el cual soporta directamente el cumplimiento de la misión institucional del SEA.

4. ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

Los roles y responsabilidades en materias de seguridad de la información, que dan cumplimiento con las directrices expuestas en la presente política general, se describen a continuación:

4.1. Comité de Seguridad de la Información (CSI)

El Servicio de Evaluación Ambiental contará con un Comité de Seguridad de la Información cuyos miembros serán designados por resolución exenta del Director/a Ejecutivo/a del SEA, y tendrá entre sus funciones la implementación de las políticas, procedimientos, normas y estándares institucionales en materias de seguridad de la información, así como también realizar reuniones y revisar la implementación de las normativas vigentes. Además, tendrá la responsabilidad de asegurar el cumplimiento de de esta política y de establecer los mecanismos de difusión en la Institución. Esta resolución debe contener el detalle de sus funciones y deberá ser publicada en el sitio colaborativo institucional en la sección de Seguridad de la Información.

4.2. Comité Operativo de Seguridad de la Información (COSI)

El Comité Operativo de Seguridad de la Información responde ante el Comité de Seguridad de la Información (CSI) y es un equipo multidisciplinario de carácter operativo cuyos miembros serán designados por resolución exenta del Director/a Ejecutivo/a del SEA. Sus responsabilidades principales son de apoyo y de consulta en materias varias de acuerdo a la función que cumplen en el Servicio, además tienen la responsabilidad de la evaluación, creación, revisión y actualización de políticas, procedimientos, planes, manuales entre otros documentos relacionados. La resolución que lo designe debe contener el detalle de sus funciones y deberá ser publicada en sitio colaborativo institucional en la sección de Seguridad de la Información.

4.3. Encargado/a de Seguridad

El Servicio de Evaluación Ambiental contará con un Encargado/a de Seguridad de la Información designado mediante resolución exenta del Director/a Ejecutivo/a del SEA, y tendrá entre sus responsabilidades la difusión de la política, la vigilancia de su cumplimiento, la aplicación de sus procedimientos y la coordinación de inducciones si fuese necesario. Esta resolución debe contener el detalle de sus funciones y deberá ser publicada en el sitio colaborativo institucional, en la sección de Seguridad de la Información.

[1] Disponible en: http://www.dipres.gob.cl/597/articles-203541_doc_pdf.pdf

4.4. La Dotación del Servicio de Evaluación Ambiental

La Dotación, entendida como las personas que desempeñan funciones en el Servicio de Evaluación Ambiental (funcionarios/as de planta, funcionarios/as a contrata, personal a honorarios o alumnos/as en práctica que preste servicios permanentes o temporales) deberán desempeñarlas cumpliendo con las políticas de seguridad, de acuerdo a los procedimientos existentes en la organización. Cabe mencionar, que las responsabilidades básicas en materias de seguridad de la información, en los casos que corresponda, quedarán descritas en los contratos y/o en los perfiles de cargo, en alguna acta o resolución especifica y en las políticas de seguridad de la información.

5. MARCO GENERAL PARA LA NORMATIVA INTERNA DE SEGURIDAD DE LA INFORMACIÓN

La normativa del SEA se podrá estructurar de la siguiente forma:

Política General de Seguridad: corresponde a la presente política.
Políticas de dominio: corresponde a las políticas que fijan los lineamientos generales para los dominios del 05 al 18 del anexo "A" de la Norma ISO 27001.
Políticas específicas: corresponde a una política concreta, que abarca uno o varios controles de seguridad de la norma antes mencionada y son complementarias a esta Política General de Seguridad de la Información.
Instructivos y Procedimientos: corresponde a la explicación detallada de las actividades a realizar para el cumplimiento de los controles asociados al mismo.
Por su parte, se declara la existencia de un documento (**MA-SGSI-01 Sistema de Gestión de Seguridad de la Información** del Servicio), que describe la conformación y funcionamiento del SGSI del Servicio.

6. AUDITORÍAS

La Institución, a través de la División de Tecnologías y Gestión de la Información, podrá realizar en cualquier momento auditorías al equipamiento computacional y tecnológico, asimismo podrá ser auditado el tráfico de red y los accesos a Internet de los funcionarios/as de la Institución, para efectos de verificar la efectividad de los controles de seguridad de la información implementados en el SEA, considerando para estos efectos lo establecido en la Ley N° 19.628 sobre de Protección de la Vida Privada. Adicionalmente, el Departamento de Auditoría Interna del SEA auditará el SGSI y los controles de la normativa vigente, conforme a lo establecido en su planificación anual.

7. EXCEPCIONES

Podrán existir casos particulares y debidamente justificados de exclusión parcial o total de la presente Política General de Seguridad de la Información, lo cual deberá ser calificado y autorizado por escrito por el Comité de Seguridad de la Información o por el Director/a Ejecutivo/a del Servicio.

8. DIFUSIÓN

La presente Política debe ser conocida por todos los funcionarios/as de la Institución, para ello es necesario contar con una difusión a través de la plataforma de intranet y/o correo electrónico.

La difusión debe ir acompañada, en la medida de lo posible, de capacitaciones permanentes en el tiempo, para lo cual la Institución podrá asignar un presupuesto anual para capacitaciones en temas de seguridad de la información de acuerdo a las políticas establecidas por el SEA. Del mismo modo, se procurará aplicar un programa de inducciones a todos los funcionarios/as nuevos que ingresen al Servicio de Evaluación Ambiental con el fin que toda la dotación se sensibilice en prevenir y proteger los activos de la información para que sea parte del quehacer de la Institución y del desarrollo de las personas.

9. FRECUENCIA DE REVISIÓN

El presente documento será sometido a revisiones cada dos años o cuando se presenten cambios a nivel estructural en la Institución, o cambios tecnológicos que impacten la seguridad de la información y deban ser abordados por las políticas generales de la Institución.

10. INCUMPLIMIENTO Y SANCIONES

El incumplimiento de la presente Política puede llegar a comprometer la continuidad de las operaciones de la Institución, asimismo, generar las responsabilidades respectivas, las que serán canalizadas de acuerdo a lo establecido en el estatuto administrativo.

Por este motivo, la Dirección Ejecutiva será quien decida las acciones a tomar en el caso de incumplimiento de la presente política o las normas de seguridad de la información.

Lo anterior, es sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso corresponda a la(s) persona(s) implicada(s) en el o los incumplimientos.

En efecto, los funcionarios/as deberán observar todo el contenido de la presente Política, pero especialmente en lo que dice relación con la fidelidad en la custodia de los documentos que en razón de su cargo les han sido confiados, so pena, en caso de incumplimiento, de generarse la correspondiente responsabilidad administrativa. De esta forma, los funcionarios/as del SEA no podrán sustraer, suprimir, revelar, destruir información que han obtenido en razón de su cargo o por cualquier causa, cualquiera sea su fuente, o elaborada por el mismo Servicio, debiendo considerar, a este respecto, las obligaciones, responsabilidades, prohibiciones y deberes inherentes al cargo reguladas por el Estatuto Administrativo o por el convenio de honorarios a suma alzada, según corresponda, todo vinculado además a los respectivos perfiles de cargo[2].

[2] Salvo, conforme lo ha dicho la Contraloría General de la República (dictamen 68.963/2009), que se trate de situaciones en las que se pueda proceder a la eliminación de documentos públicos, teniendo presente

Sin perjuicio de lo anterior, también se podrá verificar la correspondiente responsabilidad penal del funcionario/a en la medida que se cumplan los prepuestos del tipo penal respectivo. De esta forma, se deberán considerar por la jefatura correspondiente, los tipos penales establecidos en los párrafos 7 y 8 del Título V "*De los crímenes y simples delitos cometidos por empleados públicos en el desempeño de sus cargos*", específicamente, el mandato contenido en el artículo 242 del Código Penal, que sanciona al "*empleado público que substraiga o destruya documentos o papeles que le estuvieren confiados por razón de su cargo, [el que] será castigado: 1° Con las penas de reclusión menor en su grado máximo y multa de veintiuna a veinticinco unidades tributarias mensuales, siempre que del hecho resulte grave daño de la causa pública o de tercero. 2° Con reclusión menor en sus grados mínimo a medio y multa de once a veinte unidades tributarias mensuales, cuando no concurrieren las circunstancias expresadas en el número anterior*".

Al respecto, cabe agregar, que los empleados públicos, conforme a lo dispuesto en el artículo 175 letra b) del Código Procesal Penal, deben denunciar los delitos de que tomaren conocimiento en el ejercicio de sus funciones y, especialmente, en su caso, los que notaren en la conducta ministerial de sus subalternos; dentro de las veinticuatro horas siguientes al momento en que tomaren conocimiento del hecho criminal artículo 176).

11. GLOSARIO DE TÉRMINOS

Activo de información: Información o datos que poseen valor para una institución.

Dominio: Es un grupo de trabajo en red constituido con estructura jerárquica que permite compartir recursos y privilegios de acuerdo a los perfiles asignados a cada usuario.

Egreso: Se entenderá como la salida de una persona de la institución, ya sea por renuncia voluntaria, desvinculación por parte del Servicio o cualquier otra causal.

Evento de Seguridad de la Información: será todo aquel problema o inconveniente que no impacte el normal desarrollo de las operaciones del Servicio, el cual podrá considerar amenazas o riesgos asociados a los activos de información de la Institución.

Funcionario/a: Empleado/a de la organización, ya sea, planta, contrata u honorarios. También puede ampliarse a alumnos/as en práctica o externos que presten un servicio temporal.

---

que con arreglo al artículo 14, letra a), del decreto con fuerza de ley N° 5.200, de 1929, del Ministerio de Educación, Ley Orgánica de la Dirección de Bibliotecas, Archivos y Museos, deben ingresar anualmente al Archivo Nacional, los documentos a que alude ese texto legal, que hayan cumplido cinco años de antigüedad; asimismo, que la ley N° 18.845, en sus artículos 2 al 6, establece un sistema de aplicación general de microcopia o micrograbación de documentos, disponiendo que esas reproducciones tendrán el mismo valor que los originales y que estos últimos podrán destruirse una vez transcurridos 5 o 10 años desde dicho proceso; y en lo que concierne a la eliminación de formularios o elementos similares, con motivo de haber perdido éstos su utilidad, es posible recurrir a las normas de disposición de material de desecho contenidas en los artículos 31 y 32 del decreto N° 577, de 1978, del ex Ministerio de Tierras y Colonización, debiendo añadirse que al momento de eliminarse esta clase de material, debe levantarse un acta donde se individualicen los bienes que se destruyen, consignándose su denominación, la cantidad de ellos en que recae la medida y los documentos relativos a su adquisición. (Aplica dictamen N° 49.118, de 2009).

Incidente de Seguridad de la Información: es un hecho consumado, de forma intencional o no, y a la vez que, haya afectado la confidencialidad, integridad o disponibilidad de los activos y/o sistemas de información de la Institución, y sobre los cuales deben tomarse medidas correctivas inmediatas con el objeto de evitar daños mayores o reincidencias.

Información: Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.

Institución: Servicio de Evaluación Ambiental.

Medios de Procesamiento de la Información: Se refiere donde se encuentra resguardada la información en el Centro de Datos o Data Center.

Políticas: Intención y dirección general expresada formalmente por la autoridad máxima del Servicio.

Procedimientos: Métodos o sistema estructurado para cumplir un objetivo.

Proveedor: Persona que presta servicio a la Institución, ya sea contratista, subcontratista, otros.

Riesgo: Combinación de la probabilidad de ocurrencia de un evento y su impacto.

Seguridad de la Información: Es el conjunto de medidas que protegen los activos de información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio y/o minimizar el daño, de modo de preservar la confidencialidad, integridad y disponibilidad de la información.

Usuario/a: Toda persona a la cual se le da autorización para acceder a determinada información, y así poder cumplir con su trabajo en la Institución.

Tercero(s): Se refiere a todas aquellas personas, naturales o jurídicas, distintas al Servicio de Evaluación Ambiental.

Malware / Virus: Programa diseñado con el objetivo de alterar el normal funcionamiento de un equipo computacional y su software.

Visita: Persona que no presta servicio a la Institución, ya sea familiar o amigo de un funcionario/a, socios, clientes, otro.

12. REFERENCIAS BIBLIOGRÁFICAS Y NORMATIVAS

- Resolución Exenta N° 1385/2018, que “Aprueba normas para la creación y funcionamiento del Comité de Seguridad de la Información del SEA”, modificada por Resolución Exenta N° 202199101739.
- Resolución Exenta N° 1386/2018 que “Actualiza el Comité Operativo de Seguridad de la Información del SEA”.
- Resolución Exenta N° 202199101365/2021 que “Designa Encargado de Seguridad de la Información y asigna funciones”.
- Instituto Nacional de Normalización, (2013). Norma chilena Nch-ISO 27001. Santiago: INN
- Subsecretaría del Min. Del Interior, Dirección de Presupuesto del Min. Hacienda, (2015). Guía Metodológica 2015 -2019 – Indicador Transversal SSI. Santiago.
- Ley N° 18.834 que aprueba Estatuto Administrativo.

- Ley N° 20.285 sobre Acceso a la Información Pública.
- Ley N° 19.628 sobre de Protección de la Vida Privada.
- Código Procesal Penal.
- Código Penal.
- Decreto Supremo Nro. 83 del Ministerio Secretaría General de la Presidencia, (2004), sobre la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

Firmado por: Hernán Andrés Joglar Espinosa
Fecha: 07/12/2021 07:26:09 CLST

Firmado por: Iván Parra González
Fecha: 07/12/2021 10:47:44 CLST

Firmado por: Genoveva Razeto Cáceres
Fecha: 07/12/2021 11:59:41 CLST

Firmado por: Hernán Brucher Valenzuela
Fecha: 09/12/2021 21:46:13 CLST