POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

SERVICIO DE EVALUACIÓN AMBIENTAL

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 y aprobado por	Revisado y aprobado por	Aprobado por
Hugo Cabezas Contreras	Rodrigo Cerda Astorga	Camila Palacios Ryan	Valentina Durán Medina
Encargado de Seguridad de la Información	Jefe (S) División de Tecnologías y Gestión de la Información	Jefa (S) División Jurídica	Directora Ejecutiva
Fecha: Conforme a firma electrónica	Fecha: Conforme a firma electrónica	Fecha: Conforme a firma electrónica	Fecha: Conforme a firma electrónica

Nota: Este documento se encuentra firmado digitalmente en su última página.

HISTORIAL DE VERSIONES

Tabla de Identificación y Control de Cambios

Versión	Fecha	Sección	Resumen de modificaciones o motivos	Elaborado por	Revisado por
8.2	05/10/2023	1, 1.3, 2, 3 y 12	✓ Se mejora la redacción de la "Declaración Institucional". ✓ Se mejora la redacción de la "Importancia para la Institución". ✓ Se agrega "Gestión" al título del punto 2: "Objetivos del SSI". ✓ Se mejora redacción del "Alcance", referenciando links a los objetivos estratégicos de ficha de identificación definiciones estratégicas año 2023. ✓ Se actualiza referencia bibliográfica.	Hugo Cabezas C. Encargado de Seguridad de la Información	Rodrigo Cerda A. Jefe (S) División Tecnologías y Gestión de la Información Camila Palacios R. Jefa (S) División Jurídica
8.1	06/12/2022	12	• Se agrega ley 21.459 sobre delitos informáticos. • Se modifica resolución que nombra al Encargado de Seguridad de la Información, haciendo referencia a "resolución vigente".	Hugo Cabezas C. Encargado de Seguridad de la Información	Hernán Joglar E. Jefe División Tecnologías y Gestión de la Información Iván Parra G. Jefe Depto Soporte Administrativo – DJ.
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 frase "disponibilidad" a 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 Depto auditoría Eliminado.	Fernando Jofré A. Encargado de Seguridad de la Información	Hernán Joglar E. Jefe División Tecnologías y Gestión de la Información Iván Parra G. Jefe Depto. Soporte Administrativo – DJ.
7.0	14/08/2019	Todas	1. Todos los capítulos. 2. Revisión y actualización. 3. Se actualizó y simplificó alcance, en tal sentido la especificación de 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 E. Jefe División Tecnologías y Gestión de la Información Iván Parra G. Jefe Depto. Soporte Administrativo – DJ.
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 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 Jaime Guarello Abogado 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 E. Jefe División Tecnologías y Gestión de la Información Rodrigo Cerda A. Jefe Depto. Infraestructura y Operaciones Javier Herrera Abogado División Jurídica Juan Moscoso F. Jefe División Jurídica

Versión	Fecha	Sección	Resumen de modificaciones o motivos	Elaborado por	Revisado por
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 equipamiento computacional 14. Se eliminó la sección Clasificación de la información; temas fueron agregados a 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 Depto. Infraestructura y Operaciones José Adolfo Moreno Jefe 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 División Jurídica
1.0	25/07/2011	Todas	Elaboración	José Luis Sepúlveda	Carlos Pinilla M. Jefe División de Tecnologías y Gestión de la Información

INDICE DE CONTENIDO

1. DECLARACIÓN INSTITUCIONAL

Los riesgos sobre los activos de información en las organizaciones 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 a través de su "Sistema de Gestión de Seguridad de la Información - SGSI", el cual se encuentra implementado conforme a 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 la Protección de la Vida Privada y la Ley N° 18.834 que aprueba el Estatuto Administrativo.

La presente Política de Seguridad entrega las directrices respecto de la forma en que se debe implementar la seguridad de la Información conforme 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 el SEA. 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 de la Institución, cobran relevancia para los procesos del negocio, pues estos aportan valor a dichos procesos y son considerados un bien institucional; en virtud de lo anterior, 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, el "SEA", el "Servicio" o la " Institución").

En este sentido, la operación del Sistema de Gestión Seguridad de la información - SGSI, conlleva a garantizar el correcto manejo de los activos de información, de manera de gestionar sus riesgos asociados, generar mayores beneficios para las partes interesadas, incluidos los ciudadanos y evitar el uso indebido de los mismos. Por tal motivo, esta política general se presenta como una herramienta organizacional para interiorizar a la dotación del Servicio, sus colaboradores y partes interesadas, sobre la importancia y sensibilidad de la información generada al interior del Servicio, junto con dar a conocer y orientar sobre el uso de los servicios que la soportan.

2. OBJETIVOS DEL SISTEMA DE GESTIÓN 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 del Servicio 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 definido para el SGSI, actuales o futuros, por tanto, la no inclusión explícita de alguno de ellos en el presente documento no constituye argumento para no protegerlos.

Por lo anterior, el Servicio ha definido para su Sistema de Gestión de Seguridad de la Información – SGSI y en conformidad a la norma ISO/IEC 27001:2013, el siguiente alcance:

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

Este alcance constituye el proceso fundamental para garantizar la continuidad de la operación de los objetivos estratégicos institucionales[1], los cuales soportan el cumplimiento de la misión institucional.

4. ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

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

4.1. Comité de Seguridad de la Información (CSI)

El SEA contará con un Comité de Seguridad de la Información (CSI) cuyos miembros serán designados por resolución exenta del/la Director/a Ejecutivo/a del Servicio, y tendrá entre sus funciones la implementación de políticas, procedimientos, normas y estándares 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 la presente política y de establecer los mecanismos de difusión. Esta resolución debe contener el detalle de sus funciones y deberá ser publicada en el portal de colaboración del Servicio 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/la Director/a Ejecutivo/a del Servicio. Sus responsabilidades principales son de apoyo y de consulta en materias varias de acuerdo a las funciones que cumplen, 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 el portal de colaboración del Servicio en la sección de Seguridad de la Información.

[1] Disponible en https://www.dipres.gob.cl/597/articles-290505_doc_pdf.pdf

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/la 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 portal de colaboración del Servicio en la sección de Seguridad de la Información.

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 específica de seguridad de la información.

5. MARCO GENERAL NORMATIVA INTERNA DE SEGURIDAD DE LA INFORMACIÓN

La normativa del SEA se estructurará 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 políticas concretas, que abarcan uno o varios controles de seguridad de la norma ISO 27001 y complementarias a la presente Política.
- **Instructivos y Procedimientos:** Corresponde a la explicación detallada de las actividades a realizar para el cumplimiento de los controles asociados al mismo.
- **Documento de Contexto:** “Manual del Sistema de Gestión de Seguridad de la Información del SEA” (MA-SGSI-01), que describe la conformación y funcionamiento del SGSI.

6. AUDITORÍAS

El SEA, 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 la red y los accesos a Internet de los/as funcionarios/as, para verificar

la efectividad de los controles de seguridad de la información implementados en el Servicio, considerando 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 su planificación anual.

7. EXCEPCIONES

Podrán existir casos particulares y debidamente justificados de exclusión parcial o total de la presente política, lo que deberá ser calificado y autorizado en forma escrita por el Comité de Seguridad de la Información (CSI) o por el/la Director/a Ejecutivo/a del Servicio.

8. DIFUSIÓN

La presente política debe ser conocida por todos los/as funcionarios/as del SEA, para ello es necesario contar con una difusión a través del portal de colaboración del Servicio y en el sitio web oficial del SEA para las partes interesadas externas.

La difusión debe ir acompañada, en la medida de lo posible, de capacitaciones permanentes, 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 inducción a los/as funcionarios/as que ingresen al Servicio con el fin que toda la dotación se sensibilice en prevenir y proteger los activos de la información como parte del quehacer institucional y del desarrollo de las personas.

9. FRECUENCIA DE REVISIÓN

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

10. INCUMPLIMIENTO Y SANCIONES

El incumplimiento de la presente política puede llegar a comprometer la continuidad de las operaciones del SEA, 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/as funcionarios/as deberán observar todo el contenido de la presente política, especialmente 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/as 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 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].

Sin perjuicio de lo anterior, también se podrá verificar la correspondiente responsabilidad penal del/la 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).

---

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

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: Problema o inconveniente que no impacta el normal desarrollo de las operaciones, pudiendo considerar amenazas o riesgos asociados a los activos de información del Servicio.

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

Incidente de Seguridad de la Información: 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 del Servicio 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.

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 o Empresa 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: 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 riesgos, y así 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.

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

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

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

12. REFERENCIA BIBLIOGRÁFICA Y NORMATIVA

- Resolución Exenta vigente que "Aprueba normas para la creación y funcionamiento del Comité de Seguridad de la Información del SEA".
- Resolución Exenta vigente que "Actualiza el Comité Operativo de Seguridad de la Información del SEA".
- Resolución Exenta vigente que "Designa al 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.
- Ley N°21.459, establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.
- Ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley N° 17.336, sobre Propiedad Intelectual y Ley N°20.435 que la modifica.
- DS 83/2005 Ministerio Secretaría General de la Presidencia, norma técnica para Órganos de la Administración del Estado seguridad y confidencialidad de documentos electrónicos.
- DS 01/2015 del Ministerio Secretaría General de la Presidencia, sobre la norma técnica sobre sistemas y sitios web de los órganos de la administración del estado.
- DS 273/2022 del Ministerio del Interior y Seguridad Pública, establece obligación de reportar incidentes de ciberseguridad.
- Política Nacional de Ciberseguridad.
- Instructivo Presidencial N°008/2018 sobre Ciberseguridad.
- Código Procesal Penal / Código Penal.

(Hoja en blanco para firmas)

Firmado Digitalmente por hugo.cabezas hugo.cabezas
Fecha: 11-10-2023 16:14:12:580 UTC -03:00
Razón: Firma realizada por el sistema SGC
Lugar: SGC

Firmado por: Rodrigo Cerda Astorga
Fecha: 16/10/2023 17:06:49 CLST

Firmado por: Valentina Alejandra Durán Medina
Fecha: 19/10/2023 17:33:03 CLST