POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ELABORADO POR	REVISADO POR	APROBADO POR
M. Cecilia Ríos Suazo Encargada de Seguridad de la Información	Javier Espinoza Gajardo Jefe Unidad de Gestión Estratégica	Sergio Mierzejewski Lafferte Director Nacional Servicio de Registro Civil e Identificación (S)

V°B° Subdirectora Jurídica

V°B° Asesor SED

Índice

HISTORIAL DE VERSIONES

N° de Versión	Fecha	Motivo de la revisión	Páginas elaboradas o modificadas
N°0 (cero)	26/11/2014	Elaboración inicial de la política a propósito de los requisitos establecidos en la norma NCh NCh-ISO/IEC 27001:2013.	Todas
N°1 (uno)	25/5/2016	Revisión a propósito de la actualización de la norma NCh NCh-ISO/IEC 27001:2013.	Todas
N°2 (dos)	30/05/2017	Revisión anual de la política según norma NCh NCh-ISO/IEC 27001:2013.	Pág. 3 II Alcance Pág. 4 Responsabilidades en el Sistema de Seguridad de la Información.
N°3 (tres)	15/10/2018	Revisión anual de la política según norma NCh NCh-ISO/IEC 27001:2013. Incorporación de directrices de la Política Nacional de Ciberseguridad.	Portada: Actualización de firmas. Pág. 4 Se agregan las responsabilidades de la Unidad de Atención a Instituciones. Pág. 5 Punto VI puntos (d) y (e). Pág. 5 Se definen indicadores de evaluación para revisión de la política.
N°4 (cuatro)	16/09/2019	Revisión anual de la política según noma NCh ISO 27001:2013. Ajuste a estructura del documento.	Todas
N°5 (cinco)	04/11/2020	Revisión anual de la política según norma NCh NCh-ISO/IEC 27001:2013. Incorporación lineamientos NCh NCh-ISO/IEC 27701:2020 Se incorpora el concepto de Sistema de Seguridad y Privacidad de la Información.	Todas

1. DECLARACIÓN INSTITUCIONAL.

El Servicio de Registro Civil e Identificación (en adelante el SERVICIO o el SRCeI), se compromete a Gestionar la Seguridad y Privacidad de la Información para lograr niveles adecuados de confidencialidad, integridad, disponibilidad y privacidad de los activos de información que la institución considere relevante conservar. Para ello, desarrollará un trabajo paulatino de implementación de un Sistema de Seguridad y Privacidad de la Información (en adelante, SSI) basado en las Normas Chilenas NCh ISO 27.001:2013 y NCh ISO 27.701:2020, tendiente a homogeneizar los criterios de seguridad, con el objeto de preservar los activos de información de la Institución con respecto a:

a) **Confidencialidad**: El SRCeI deberá velar porque se apliquen los controles necesarios para resguardar los activos de información y tratar los riesgos asociados, por ejemplo, de cualquier acceso libre o no autorizado, revelaciones accidentales, espionaje, violación de la privacidad y otras acciones de similares características.

b) **Integridad**: El SRCeI deberá velar porque se apliquen los controles necesarios para resguardar los activos de información y tratar los riesgos asociados, por ejemplo, de cualquier degradación por efectos de agentes internos o externos, ambientales o manipulación que afecten su exactitud y completitud.

c) **Disponibilidad**: El SRCeI deberá velar porque se apliquen los controles necesarios para resguardar los activos de información y tratar los riesgos asociados, por ejemplo, de cualquier interrupción, asegurando que se encuentren accesibles y utilizables, para que no afecte la continuidad operacional.

d) **Privacidad**: El SRCeI deberá velar porque se apliquen los controles necesarios para proteger los activos de información a fin de resguardar adecuadamente la privacidad de los datos personales de los usuarios y usuarias mantenidos en los registros a su cargo.

La Gestión de la Seguridad y Privacidad de la Información, será clave para identificar y tratar los riesgos que afecten la continuidad operacional de la Institución, sus relaciones e imagen con la ciudadanía, los proveedores y sus funcionarios y funcionarias.

2. INTRODUCCIÓN DE LA POLÍTICA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La información corresponde a un activo del SRCeI, el cual está expuesto a riesgos y amenazas dinámicas, que pueden provenir desde dentro o fuera de la organización, y pueden ser intencionales o accidentales. Su ocurrencia puede provocar pérdidas materiales y económicas, daños en la imagen institucional y en la confianza de los clientes, infracciones legales, incumplimiento regulatorio, vulneración de derechos de funcionarias y funcionarios o de terceros. Por lo cual, es importante proteger adecuadamente los activos de información del Servicio de Registro Civil e Identificación.

Toda información del SRCeI, independiente de la forma en que se documente (soporte), debe ser protegida adecuadamente a través de la implementación de un conjunto de controles (Anexo A norma NCh-ISO/IEC 27001:2013 y Anexos A y B norma NCh-ISO/IEC 27701:2020), que se definen en políticas, normas y procedimientos de Seguridad y Privacidad de la Información.

En vista de lo anterior, la alta dirección del Servicio de Registro Civil e Identificación declara su intención de apoyar los objetivos estratégicos de Seguridad y Privacidad de la Información, velando que se encuentren alineados con las estrategias y los objetivos propios del negocio.

3. OBJETIVOS POLÍTICA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los objetivos de la Política de Seguridad y Privacidad de la Información se encuentran alineados con el Sistema de Seguridad y Privacidad de la Información y corresponden a:

1) Minimizar el riesgo en los procesos asociados a la seguridad de la información y privacidad de datos.

2) Cumplir con los principios de seguridad de la información y la privacidad de los datos.

3) Proteger todos los activos de la información de la Institución.

4) Establecer políticas, procedimientos e instructivos que refuercen los procesos contenidos en el Sistema de Seguridad y Privacidad de la Información.

5) Fortalecer la cultura de seguridad de la información en los trabajadores y proveedores.

6) Apoyar las garantías de la continuidad del negocio frente a incidentes de seguridad y privacidad de la información.

4. ALCANCE DE LA POLÍTICA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La presente política tiene como alcance el Sistema de Seguridad y Privacidad de la Información, debiendo ser cumplida por todas las partes que se relacionen directa o indirectamente con los procesos de seguridad y privacidad de la información del SRCel de forma interna o externa.

Con todo, la presente Política deberá ser aplicada y cumplida por **todos(as) los(as) funcionarios(as)** de planta y a contrata, así como aquellos que se encuentren en calidad de suplente o reemplazo; al personal contratado a honorarios, Código del Trabajo, y a los terceros (incluyendo contratistas) que interactúen de manera habitual u ocasional con la institución.

5. ESTRUCTURA DE POLÍTICAS, NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

Los controles de la Norma corresponderán a aquellos establecidos en NCh-ISO/IEC 27001:2013 y NCh-ISO/IEC 27701:2020, los que serán aplicados con el objetivo de resguardar todos aquellos procesos que pudiesen poner en riesgo los activos de la información y a su vez la protección de datos personales.

A partir de las Políticas se desarrollarán procedimientos e instructivos de trabajo, que serán la guía para la ejecución de actividades de seguridad y privacidad de la información al interior de SRCel.

5.1. Controles NORMA NCh-ISO/IEC 27001:2013

Se consideran los 144 controles de la norma contenidos y distribuidos en los siguientes dominios:

A.5 Políticas de Seguridad de la Información.
A.6 Organización de la seguridad de la Información.
A.7 Seguridad de los Recursos Humanos.

A.8 Administración de Activos.
A.9 Control de Acceso.
A.10 Criptografía.
A.11 Seguridad Física y Ambiental.
A.12 Seguridad de las Operaciones.
A.13 Seguridad en las Comunicaciones.
A.14 Adquisición, desarrollo y mantenimiento de sistemas.
A.15 Relaciones con los proveedores.
A.16 Administración de incidentes de seguridad de la información.
A.17 Aspectos de la seguridad de la información de la administración de la continuidad comercial.
A.18 Cumplimiento.

5.2. Controles NORMA NCh-ISO/IEC 27701:2020

Se consideran los 49 controles de la norma contenidos y distribuidos en los siguientes dominios:

A.7.2 Condiciones para la recopilación y el procesamiento
A.7.3 Obligaciones respecto de los titulares de PII
A.7.4 Privacidad desde el diseño y por defecto
A.7.5 Intercambio, transferencia y eliminación de PII
B.8.2 Condiciones para la recopilación y el procesamiento
B.8.3 Obligaciones respecto de los titulares de PII
B.8.4 Privacidad desde el diseño y por defecto
B.8.5 Intercambio, transferencia y eliminación de PII

6. TRATAMIENTO DE DATOS

Para el tratamiento de datos, el Servicio de Registro Civil e Identificación, se rige bajo las recomendaciones y buenas prácticas sugeridas por el Consejo para la Transparencia sobre la protección de datos personales.

Los datos serán clasificados de la siguiente manera:

a) **Datos de carácter personal:** Los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. (Art. 2, letra f) Ley Nº 19.628 Sobre Protección de la Vida Privada). El tratamiento de estos datos sólo puede efectuarse cuando esta ley u otras disposiciones

legales lo autoricen o el titular consienta expresamente en ello (Art. 4, Ley N° 19.628 Sobre Protección de la Vida Privada).

b) **Datos sensibles:** Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual (Art.2, letra g), Ley Nº 19.628 Sobre Protección de la Vida Privada). En virtud de lo establecido en el Artículo 7, inciso 2° de la letra i) de la Ley Nº 20.285, se entienden datos sensibles estos mismos mencionados, pero en vez de origen racial, se indica origen social.

Sobre las fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes, su consulta debe poder ser realizada por cualquier persona, como, por ejemplo, los contenidos en diarios o en medios de comunicación social.

Los datos personales de los(as) usuarios(as) son recopilados a través de las actuaciones que el SRCeI tiene disponibles a través de sus distintas plataformas, esto es: oficinas presenciales, Oficina Internet, módulos de trámites y servicios en línea del sitio web institucional (www.registrocivil.cl), portal Gobierno Transparente, quioscos de autoatención y aplicaciones móviles, los que son utilizados solo dentro de la competencia y atribuciones que tiene el SRCeI.

Los datos personales de los usuarios(as) son recolectados, almacenados, usados y puestos en circulación según requerimientos del consultante y conforme a lo dispuesto en la Ley N°19.628, Sobre Protección de la Vida Privada, y los cuerpos legales que correspondan a la materia en particular.

6.1 Procedimientos para el tratamiento de los datos personales

En cuanto a los registros o banco de datos, estos son clasificados como:

a) Registros automatizados: todo conjunto de datos de carácter personal que para su tratamiento han o están sujetos al uso de herramientas tecnológicas específicas, en los procesos de acceso, recuperación o tratamiento.

b) Registros no automatizados: todo conjunto de datos de carácter personal organizado de forma manual, contenido en registros manuales, impresos,

sonoros, magnéticos, visuales u holográficos, y estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales.

Es responsable de los registros o bancos de datos (según las buenas prácticas sugeridas por el Consejo para la Transparencia) el SRCeI, de acuerdo con las competencias que la normativa establezca sobre las decisiones relacionadas con el tratamiento de datos de carácter personal.

La protección de datos debe estar basada en los siguientes principios:

A. Principio de licitud.
B. Principio de calidad de los datos, esto es:
    i. Principio de veracidad.
    ii. Principio de finalidad.
    iii. Principio de proporcionalidad.
C. Principio de Información.
D. Principio de seguridad.
E. Principio de confidencialidad o secreto.

Conforme a lo dispuesto en el artículo 19 N°4 de la Constitución Política de la República y a las normas pertinentes de la Ley N° 19.628 sobre protección de la vida privada y sus modificaciones posteriores, el SRCeI, efectúa tratamiento de datos personales a través de sus distintas plataformas de atención, presenciales o virtuales; en función de lo establecido en los Artículos 3° y 4° de la Ley N°19.477.

6.2 Titular de los Datos Personales.

Los datos personales se asocian a una persona individual, denominada “titular”. Esta persona tiene derecho a conocer:

a) Información de los bancos de datos de responsabilidad del SRCeI, del fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende.

b) Información sobre datos relativos a su persona, procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

c) La modificación de sus datos personales en caso de que éstos sean erróneos, inexactos, equívocos o incompletos, y así se acredite.

d) La eliminación de los datos personales entregados cuando su almacenamiento carezca de fundamento legal o cuando estuvieran caducos.

e) La eliminación o bloqueo de los datos personales, en aquellos casos en que haya proporcionado voluntariamente sus datos personales y no desee continuar figurando en el registro respectivo, sea de manera definitiva o temporal.

6.3 Deberes del Responsable del tratamiento de los datos personales

El Responsable del Tratamiento de Datos Personales, en este caso el SRCeI, debe cumplir con los siguientes deberes:

a) Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento.

c) Garantizar que la información que suministre el encargado del tratamiento de los datos, esto es - en el caso del SRCeI- la jefatura del Registro correspondiente sea veraz, completa, exacta, actualizada, comprobable y comprensible.

d) Actualizar la información, correspondiente al registro a su cargo, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada se mantenga actualizada.

Es importante señalar que, pertenecen al SRCeI todos aquellos datos contenidos y/o publicados en su sitio web institucional (www.registrocivil.gob.cl), intranet

institucional, aplicaciones móviles, así como aquellos datos que hayan sido recolectados por funcionarios(as) del SRCeI o por terceros contratados por ella en cualquiera de sus plataformas de atención, presenciales o virtuales.

Los contenidos de acceso público disponibles en www.registrocivil.gob.cl pueden ser utilizados por el usuario(a) para fines no comerciales.

7 MARCO LEGAL, REGULATORIO Y NORMATIVO

a) **Norma NCh-ISO/IEC 27001:2013.** Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos.

b) **Norma NCh-ISO/IEC 27701:2020.** Técnicas de seguridad – Extensión NCh-ISO/IEC 27001 e NCh-ISO/IEC 27002 para la gestión de la información de privacidad – Requisitos y directrices.

c) **Norma NCh-ISO/IEC 27002:2015.** Tecnologías de la Información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información

d) **Ley 17.336, sobre Propiedad Intelectual**: En sentido amplio, la propiedad intelectual dice relación con toda creación que produce la mente humana; esto es los inventos, modelos de utilidad, marcas, obras literarias y artísticas, etc. La Propiedad Intelectual comprende, la Propiedad Industrial y el Derecho de Autor (Instituto Nacional de Propiedad Industrial INAPI). La Ley busca proteger los derechos que, por el solo hecho de la creación de la obra, adquieren los autores de esta, cualquiera que sea su forma de expresión, y los derechos conexos que ella determina.

e) **Ley 19.223, Ley de Delitos Informáticos:** Tiene por finalidad proteger la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan. (Historia Fidedigna de la Ley, Primer Trámite Constitucional, Cámara de Diputados, Moción Parlamentaria año 1991)

f) **Ley 19.477, que Aprueba Ley Orgánica del Servicio de Registro Civil e Identificación:** Su artículo 3° señala que “El Servicio velará por la constitución legal de la familia y tendrá por objeto principal registrar los actos

y hechos vitales que determinen el estado civil de las personas y la identificación de estas.

Le corresponderá, también, llevar los registros y efectuar las actuaciones que la ley encomiende."

g) **Ley 19.628, Ley de Protección de la Vida Privada:** Establece un conjunto de principios y derechos relativos al manejo de datos personales en el país que puede exigir un titular de datos personales a quien posea o administre un registro de estos, junto con reglas de aplicación general para el manejo de datos personales por el sector público y privado, en torno al resguardo de la confidencialidad de esa información.

h) **Ley 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma:** Regula el uso de documentos electrónicos en el país y, con ello, mecanismos para asegurar la integridad y confidencialidad de la información, mediante el uso de mecanismos de firma digital, junto con un sistema que garantice el apropiado funcionamiento de quienes prestan estos servicios.

i) **Ley 20.285, sobre Acceso a la Información Pública**: Crea un régimen de transparencia para las actividades del Estado, con obligaciones de transparencia activa, que debe efectuarse a través del sitio web de cada organismo público afectado; y pasiva, consistente en los datos que puede requerir cualquier persona a estos organismos, en la medida que no afecte otros derechos e intereses establecidos en la ley, como la seguridad del Estado o la privacidad de terceros, de manera tal que no se afecte la confidencialidad de la información en juego.

j) **Decreto N°83, Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos**: Establece la Norma Técnica sobre seguridad y confidencialidad del documento electrónico.

8 ROLES Y RESPONSABILIDADES

8.1 Roles.

El SRCeI contará con una estructura funcional para administrar el Sistema de Seguridad y Privacidad de la Información (SSI), constituida por los siguientes roles:

a) Director/a Nacional,

b) Comité Directivo de Seguridad y Privacidad de la Información (CDS),

c) Comité Operativo de Seguridad y Privacidad de la Información (COS),

d) Encargado/a de Seguridad de la Información (ESI),

e) Jefe Unidad Control de Riesgos y Seguridad,

f) Encargado de Ciberseguridad,

g) Oficial de Seguridad TI,

h) Encargados/as de Seguridad de la Información Regionales.

8.2 Responsabilidades.

Rol	Responsabilidad
Director(a) Nacional	• Proveer los medios para la implementación de esta Política. • Aprobar las versiones actualizadas de esta Política.
Comité Directivo de Seguridad y Privacidad de la Información (CDS)	• Revisar, aprobar y difundir las políticas de seguridad. • Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes de seguridad. • Promover la difusión y apoyo a la Seguridad de la Información.
Comité Operativo de Seguridad y Privacidad de la Información (COS)	• Proponer al Comité Directivo de Seguridad de la Información del Servicio de Registro Civil e Identificación, nuevas políticas de seguridad de la información. • Supervisar la implementación de procedimientos e instructivos que tengan lineamientos desde las políticas de seguridad de la información.

Rol	Responsabilidad
	• Identificar los riesgos a los cuales se encuentran expuestos los activos de información, definir estrategias y proponer al Comité Directivo de Seguridad de la Información, un Plan para su tratamiento y mitigación.
Encargado(a) de Seguridad y Privacidad de la Información (ESI)	• Asesorar, coordinar y apoyar al SRCeI en materias relativas al Sistema de Seguridad y Privacidad de la Información. • Difundir y sensibilizar respecto de la Seguridad y Privacidad de la Información a los funcionarios(as) del SRCeI. • Gestionar los riesgos asociados a los activos de información del Servicio.
Jefe Unidad Control de Riesgos y Seguridad	• Generar la definición y materialización de los planes de corto, mediano y largo plazo relativos a la seguridad y privacidad de la información, desde el punto de vista de tecnologías de la información. • Asesorar al ESI en materias de riesgo y seguridad TI. • Realizar un trabajo coordinado con el Oficial de Seguridad TI.
Encargado(a) de Ciberseguridad	• Gestionar la seguridad informática del Servicio y los riesgos asociados a la Ciberseguridad. • Asesorar al ESI en materias de riesgo y ciberseguridad.
Oficial de Seguridad TI	• Prestar asesoría técnica especializada al ESI, al Subdirector(a) de Estudios y Desarrollo y al Director/a Nacional en las materias relativas a la seguridad de los Sistemas Informáticos y Documentos Electrónicos. • Realizar un trabajo coordinado con el Jefe Unidad Control de Riesgos y Seguridad.
Encargados(as) de Seguridad y Privacidad de la Información	• Asesorar al Director(a) Regional y a todos los funcionarios y funcionarias de la región, respecto del alcance de las Políticas y normas internas asociadas a la Seguridad y Privacidad de la Información.

Rol	Responsabilidad
Regionales	• Informar a ESI, cualquier acto anómalo detectado sobre el tratamiento de los activos de información.
Encargado del Tratamiento de Datos	• La jefatura encargada de un Registro en particular debe aplicar los controles adecuados para resguardar los activos de información a su cargo y la privacidad de los datos personales de los titulares.
Responsable del Tratamiento de Datos	• El responsable del tratamiento de los datos contenidos en los registros a su cargo es el propio Servicio de Registro Civil e Identificación; para lo cual se aplica la estructura descrita en la presente política

Un mayor detalle de las responsabilidades y funciones de la estructura del Sistema de Seguridad y Privacidad de la Información se encontrarán descritas en sus respectivos actos administrativos de creación y/o designación.

Además, será responsabilidad individual inexcusable de los funcionarios(as) de calidad jurídica: titular, contrata, suplencia y/o reemplazo, personal a honorarios y terceros contratados que prestan servicios, que tengan acceso a los activos de información del SRCeI, o que tengan acceso al uso de las tecnologías de la información y sus actividades en Internet, dar cumplimiento a la presente Política y a otras políticas, procedimientos o instructivos asociados al Sistema de Seguridad y Privacidad de la Información.

Las jefaturas y/o dueños de activos o procesos, deben velar porque el personal de su dependencia conozca y cumpla la presente Política y otras políticas, procedimientos o instructivos asociados al Sistema de Seguridad y Privacidad de la Información.

La jefatura de la Unidad de Gestión Estratégica debe revisar la actualización de esta Política, previo a la aprobación final por parte de la Dirección Nacional.

9 DIFUSIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El SRCeI mantendrá a disposición de los funcionarios/as y personal que se desempeñe en él, la versión actualizada de la presente política. Para estos efectos,

el documento estará disponible y publicado en el sitio web del Sistema de Gestión Integral de Calidad del SRCeI, específicamente, en la Documentación del Proceso de Seguridad de la Información, cuya URL es la siguiente http://calidad.srcei.cl/qsm/; asimismo se publicará en el sitio web institucional, en la sección “Política de Seguridad y Privacidad”.

10 VIGENCIA Y REVISIÓN

La presente política será evaluada y revisada al menos una vez al año por el Encargado/a de Seguridad de la Información, o cuando el Comité Directivo de Seguridad y Privacidad de la Información lo requiera, para asegurar su continuidad e idoneidad, considerando cambios externos o internos que puedan afectarla.

Al evaluar la efectividad y adecuación de la presente política, es necesario tener en cuenta los siguientes criterios:

a) Cambios legales y/o normativos que puedan afectar la presente Política,

b) Eventos de seguridad que afecten la Confidencialidad, Integridad, Disponibilidad o Privacidad de los activos de información.

En cuanto a los objetivos específicos a cumplir por parte del SRCeI en materias de Ciberseguridad y de Seguridad y Privacidad de la Información y Datos Personales, se determinarán en base a un análisis de los riesgos y amenazas a los que estén expuestos los activos de información críticos, por parte del Comité Directivo de Seguridad y Privacidad de la Información.

La presente versión sustituye completamente a todas las precedentes, de manera que este sea el único documento válido de entre todos los de la serie. Lo anterior, una vez que sea aprobado por el respectivo acto administrativo.

11 SANCIONES POR INCUMPLIMIENTO

El incumplimiento de la presente Política y otras políticas, procedimientos o instructivos asociados al Sistema de Seguridad y Privacidad de la Información ya sea por parte del personal del SRCeI o de externos, podrá traer como consecuencia la aplicación de las sanciones administrativas, civiles o penales establecidas en la legislación vigente y en los procedimientos internos de la institución.

Adicionalmente, acarreará para los funcionarios(as) las sanciones que correspondan, conforme a los procedimientos que se adopten. Respecto del personal a honorarios, y en resguardo de la probidad administrativa que debe concurrir en ellos, pueden ser objeto de término anticipado de su contrato. En el caso de los terceros externos, el Director Nacional enviará una carta dirigida al Coordinador General del Contrato respectivo o Representante Legal de la empresa al cual pertenece la persona infractora.

Es deber de todo el personal del SRCeI y de los terceros externos, informar a la brevedad a su jefatura directa si se tiene conocimiento del incumplimiento de la normativa vigente en esta materia. Esta información deberá canalizarse al Encargado/a de Seguridad de la Información a través de los medios formales que se tenga disponible.

12 DEFINICIONES

Término	Definición
Activo de Información	Es todo activo que tenga valor y es importante para el SRCeI, sean: documentos, sistemas, base de datos, infraestructura o personas. Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. Se distinguen tres niveles: • La Información propiamente tal, en sus múltiples formatos (papel, digital, base de datos, 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	Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema, datos o proceso.
Buen Uso	Se entiende por “buen uso” de los activos de información, las expectativas que el SRCeI tiene con respecto al cuidado que su personal debe tener con los activos que el SRCeI les entregue para el desempeño de sus funciones.
Comité de Seguridad y Privacidad	Es el equipo conformado por personal de las áreas de la institución, responsable de la toma de decisiones en temas de la seguridad y privacidad de la información.

Término	Definición
	En el caso del SRCeI, se cuenta con un Comité Directivo de Seguridad y Privacidad de la Información y un Comité Operativo de Seguridad y Privacidad de la Información.
Confidencialidad	Obligación de mantener reserva de la información del SRCeI a la que se acceda y que será exigible a cualquier persona natural o jurídica que interactúe o se relacione con el SRCeI bajo cualquier modalidad o vínculo jurídico contractual.
Dato Personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Dato Público	Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad.
Dato Sensible	Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación.
Declaración de aplicabilidad	Documento que enumera los controles aplicados por el Sistema de Seguridad y Privacidad de la Información de la Institución tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
Disponibilidad	Propiedad de la información según la cual es accesible y utilizable oportunamente por las personas o sistemas o procesos autorizados, en el formato requerido para su procesamiento.
Encargado/a de Seguridad y Privacidad de la Información (ESI)	Es la persona que la autoridad máxima designa para la definición, diseño, implementación y supervisión de las medidas de seguridad y privacidad de la información.
Encargado del Tratamiento de Datos	Persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. En el caso del SRCeI, este rol corresponde a la jefatura o encargada del Registro en cuestión, conforme lo establecido en el punto 6.3 de este documento.
Evento de Seguridad y Privacidad de la Información	Actividad o serie de actividades sospechosas que amerita ser analizada desde la perspectiva de la Seguridad y privacidad de la Información.

Término	Definición
Incidente de Seguridad y Privacidad de la Información	Evento o serie de eventos de Seguridad y privacidad de la Información, no deseados o inesperados, que compromete la Seguridad de la Información y amenaza la operación del negocio.
Integridad	Propiedad de la información según la cual sólo puede ser modificada, agregada o eliminada por las personas o sistemas autorizados para cada proceso, de tal forma de salvaguardar la exactitud y completitud de los activos de información.
Norma	Disposición de carácter general que define los lineamientos de implementación de la seguridad y privacidad de la información, estableciendo obligaciones, restricciones, prohibiciones u otras conductas esperadas.
Oficial de Seguridad de Tecnologías de la Información TI	Persona encargada de prestar asesoría técnica especializada al Encargado(a) de Seguridad de la Información, al Director(a) Nacional y al Subdirector de Estudios y Desarrollo, en materias relativas a seguridad de Sistemas Informáticos y Documentos Electrónicos.
Política	Directriz u orientación general expresada formalmente por la Alta Dirección del servicio.
Procedimiento	Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad y Privacidad de la Información.
Responsable de la Información y Privacidad de los datos	Es el usuario a cargo de la información, privacidad y de los procesos que la manipulan sean estos manuales o sistémicos.
Responsable del Tratamiento de los datos	Persona natural o jurídica, pública o privada, que por sí misma o en asociación con otros, decida sobre la base de datos y/o el Tratamiento de los datos. En este caso el SRCel.
Riesgo	Efecto de la incertidumbre. Con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos cambios en las circunstancias) y la probabilidad asociada de que ocurra.
Riesgo Residual	Los tratamientos del riesgo, a pesar de un cuidadoso diseño e implementación, pueden no producir los

Término	Definición
	resultados esperados y puede producir consecuencias no previstas.
Sistema de gestión de Seguridad de la Información (SGSI)	El SGSI es el principal concepto sobre el que se conforma la norma ISO 27001. La gestión de la Seguridad de la Información se debe realizar mediante un proceso sistémico, documentado y conocido por toda la Institución. En el caso del SRCeI, éste forma parte del Sistema de Seguridad y Privacidad de la Información.
Sistema de gestión en Privacidad de la Información (SGPI)	El SGPI (Sistema de Gestión de Privacidad de la Información) es el sistema en el que se integra la gestión eficaz de la privacidad incorporando requisitos adicionales para el procesamiento de datos personales. En el caso del SRCeI, éste forma parte del Sistema de Seguridad y Privacidad de la Información.
Sistema de Seguridad y Privacidad de la Información	Sistema adoptado por el SRCeI, para gestionar tanto la seguridad de la información como la privacidad de los datos personales de los usuarios(as), que conforman los Registros que la institución tiene a su cargo.
Tercero	Se refiere a empresas prestadoras de servicios, contratistas, subcontratistas, y sus trabajadores o personal bajo subordinación, y cualquiera que, por cuenta propia o de terceros, desarrolle trabajos para o por cuenta de la Institución.
Titular	Persona natural o jurídica cuyos Datos Personales sean objeto de Tratamiento.
Funcionario(a) / Trabajador(a)	Toda persona que tenga un vínculo contractual de trabajo con SRCeI, independiente de la calidad jurídica: Planta, Contrata, Honorario, Código del Trabajo.
Tratamiento	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
Vulnerabilidad	Debilidad de un activo o grupo de activos que puede ser materializada por una o más amenazas.