Subsecretaría de Previsión Social

Gobierno de Chile

Subsecretaría de Prevención Social

3 0 MAY 2023

TOTALMENTE TRAMITADO

APRUEBA CONVENIO DE COLABORACIÓN ENTRE LA SUBSECRETARÍA DE PREVISIÓN SOCIAL Y EL SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN.

RESOLUCIÓN EXENTA N° 57.-

SANTIAGO, 30 de mayo de 2023.

VISTOS:

Lo dispuesto en el D.F.L. Nº 1/19.653, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en el Decreto con Fuerza de Ley Nº 25, de 1959, del Ministerio de Hacienda; en las Resoluciones N°7 de 2019 y N°14 de 2022, de la Contraloría General de la República, sobre exención del Trámite de Toma de Razón; en la Resolución Afecta N° 03 de 2022, de la Subsecretaría de Previsión Social; en la Resolución Exenta N° 173 de 2023, de la Subsecretaría de Previsión Social; en la Resolución Exenta N° 44 de 2022, de la Subsecretaría de Previsión Social; y

CONSIDERANDO:

1. Que, desde el año 2022, el Ministerio del Trabajo y Previsión Social, a través de la Subsecretaría de Previsión Social, lleva a cabo la Encuesta de Protección Social (EPS), la que es un estudio tipo panel que indaga en las materias relativas a la protección social, sirviendo como almacenamiento para el diagnóstico, desarrollo y evaluación de políticas públicas en este ámbito.

2. Que, la Encuesta de Protección Social es la mayor encuesta panel en Chile, con una muestra aproximada de 20.000 personas distribuidas en todas las regiones del país.

3. Que, mediante Resolución Afecta N° 03 de 2022, se llamó a licitación pública y se aprobaron las bases administrativas, técnicas y anexos para la contratación del Servicio de Reconceptualización de Objetivos, Actualización del Cuestionario, Diseño Muestral, Trabajo de Campo, Procesamiento y Análisis de Resultados de la VIII ronda de la EPS, la que fue adjudicada mediante Resolución Exenta N° 173 de 2022.

4. Que, el Servicio de Registro Civil e Identificación, cuenta con datos, bajo la modalidad de un servicio fuera de línea, esto es, servicio batch, que contiene la información de contacto de la población del país.

5. Que, para la ejecución de la VII ola o Ronda de la Encuesta de Protección Social, es necesario contar con la información nominada de contacto más actualizada que posea el Servicio de Registro Civil e Identificación, para la correcta ejecución de la EPS.

Subsecretaría de Previsión Social

Gobierno de Chile

6. Que, atendido lo anterior, con fecha 02 de mayo de 2023, la Subsecretaría de Previsión Social y el Servicio de Registro Civil e Identificación, suscribieron un Convenio de Colaboración de entrega de información de datos fuera de línea.

7. Que corresponde a la autoridad administrativa adoptar las medidas y celebrar los actos y convenios que resguarden el normal y correcto funcionamiento de la administración y que le permitan cumplir eficazmente sus objetivos, tareas y actividades permanentes y asegurar la continuidad de sus funciones.

R E S U E L V O:

APRUÉBASE el Convenio de Colaboración de entrega de información de datos de Registro Civil fuera de línea entre la **SUBSECRETARÍA DE PREVISIÓN SOCIAL** y el **SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN,** suscrito con fecha 02 de mayo del año 2023, cuya copia se adjunta formando parte integrante de la presente resolución para todos los efectos legales.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE

CONSUELO MALDONADO HERRERA
SUBSECRETARIA DE PREVISIÓN SOCIAL (S)

KSC/DRL/JEFD

Subsecretaría de Previsión Social

Gobierno de Chile

Santiago, 30 de mayo de 2023.

MEMORANDUM N° 03/2023

DE : SUBSECRETARIA DE PREVISIÓN SOCIAL (S)

A : SR. LUIS FIGUEROA MEDIZAVAL
Profesional de la Unidad de Observatorio Previsional

SRA. GABRIELA ARTEAGA BROUSET
Profesional de la Unidad de Observatorio Previsional

Informo a usted que, mediante Resolución N° 57 de 2023, de la Subsecretaría de Previsión Social, se aprobó el convenio de colaboración de fecha 02 de mayo de 2023, suscrito entre esta Institución y el Servicio de Registro Civil e Identificación.

Se hace presente que, la cláusula séptima del contrato en cuestión establece las limitaciones en el uso de la información, la que deberá ser utilizada solo para los fines propios del convenio, debiendo procurar los funcionarios que tengan acceso a ella a velar por la confidencialidad correspondiente, en el marco del desempeño de las actividades propias de su cargo, quedando prohibido su uso en un sentido distinto, tomando las medidas necesarias para evitar que otros funcionarios no autorizados tengan acceso a ella.

Que, en consecuencia, les queda estrictamente prohibido copiar total o parcialmente, como, asimismo, revelar, publicar, difundir, vender ceder, reproducir, interferir, interceptar alterar, modificar, dañar, inutilizar, destruir, en todo o parte la información a la que tengan acceso en la ejecución del referido convenio, ya sea durante su vigencia o después de su término.

Asimismo, deberán velar por el estricto cumplimiento de las normas establecidas en la ley N° 19.628 sobre Protección a la Vida Privada, y garantizar que durante la ejecución de este convenio no se infrinjan las normas relativas al tratamiento de datos personales.

Finalmente, cumplo con hacer presente, que el incumplimiento de la presente instrucción podría acarrear responsabilidad, en los términos del Estatuto Administrativo.

REPÚBLICA DE CHILE
MINISTERIO DEL TRABAJO Y PREVISIÓN SOCIAL
SUBSECRETARÍA DE PREVISIÓN SOCIAL

CONSUELO MALDONADO HERRERA
SUBSECRETARIA DE PREVISIÓN SOCIAL (S)

DRL/PTD

C.C.:
- Unidad de Atención de Instituciones del Servicio de Registro Civil e Identificación, correo electrónico: convenios@registrocivil.gob.cl
- Dirección de Estudios Previsionales, Subsecretaría de Previsión Social.
- Sr. Luis Figueroa Mendizábal, profesional de la Unidad de Observatorio Previsional de la Subsecretaría de Previsión Social.
- Sra. Gabriela Arteaga Brouset, profesional de la Unidad de Observatorio Previsional de la Subsecretaría de Previsión Social.

Servicio de Registro Civil e Identificación
Ministerio de Justicia y Derechos Humanos
Gobierno de Chile

UAI ORD.: Nº106/2023/

ANT.: No hay.

MAT.: Remite ejemplar de Convenio Firmado.

SANTIAGO, 22 de mayo de 2023

A través de la presente, me es grato remitir a usted, un (1) ejemplar del Convenio de Colaboración de Entrega de Información de Datos de Registro Civil Fuera de Línea, suscrito con fecha 02 de mayo de 2023.

Junto a lo anterior, cumplo con hacer entrega de una copia de los siguientes documentos: Política de Seguridad y Privacidad de la Información del Servicio de Registro Civil e Identificación, versión 07; Política de Convenios con Instituciones Externas, versión 04; Política de Controles Criptográficos, versión 04; y la Política de Protección de Datos Personales para la Transferencia o Verificación de Datos a Terceros, versión 00.

Por otra parte y en virtud de lo establecido en nuestro Convenio, particularmente, respecto de la cláusula de Limitaciones en el Uso de la Información, agradeceré enviar a nuestra Unidad en formato PDF y al correo convenios@registrocivil.gob.cl, copia de la instrucción a los funcionarios de vuestra Institución que tienen acceso a la información, respecto de la imposibilidad absoluta de copiar total o parcialmente, como asimismo, revelar, publicar, difundir, vender, ceder, reproducir, interferir, interceptar, alterar, modificar, dañar, inutilizar, destruir, ya sea durante la vigencia del convenio como después de su término.

Finalmente, es de vuestra responsabilidad como Institución, proteger y resguardar la confidencialidad de la información a la que tendrá acceso, conforme a la suscripción del citado convenio.

Saluda atentamente,

REGISTRO CIVIL E IDENTIFICACIÓN
UNIDAD DE ATENCIÓN DE INSTITUCIONES
CHILE

ANDREA MUÑOZ CONTRERAS
Jefa Unidad de Atención de Instituciones

SEÑOR
CARLOS OSORIO MUÑOZ
JEFE DE UNIDAD DE OBSERVATORIO PREVISIONAL
SUBSECRETARIA DE PREVISIÓN SOCIAL

RHC
DISTRIBUCIÓN:
La indicada.
cc.: La citada.
Unidad Atención a Instituciones.
Ref.: Ticket # 49147

CONVENIO DE COLABORACIÓN
DE ENTREGA DE INFORMACIÓN DE DATOS DE REGISTRO CIVIL
FUERA DE LÍNEA ENTRE
LA SUBSECRETARÍA DE PREVISIÓN SOCIAL Y
EL SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN

En Santiago de Chile, a 02 de mayo de 2023, entre la Subsecretaría de Previsión Social en adelante **LA SUBSECRETARÍA,** RUT N°61.503.000-7, representada por su Subsecretario de Previsión Social, don Christian Larraín Pizarro, RUN N°7.015.275-4, ambos domiciliados en Huérfanos N°1273, comuna de Santiago y el Servicio de Registro Civil e Identificación, en adelante **EL SERVICIO**, RUT Nº61.002.000-3, representado por su Director Nacional, don Omar Morales Márquez, RUN Nº10.036.787-4, ambos domiciliados en Avenida Libertador Bernardo O´Higgins N°1449, Edificio Santiago Downtown, Torre 4, Piso 21, comuna de Santiago, se ha acordado lo siguiente:

PRIMERO: Antecedentes legales.

El presente Convenio se suscribe de conformidad a lo dispuesto en el D.F.L. Nº1/19.653 que fija Texto Refundido, Coordinado y Sistematizado de la Ley Nº18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; a lo dispuesto en el artículo 7°, letra i) de la Ley Nº19.477, Orgánica del Servicio de Registro Civil e Identificación; a lo dispuesto en la Ley N°19.880 que Establece Bases de los Procedimientos Administrativos que Rigen Los Actos de los Órganos de la Administración del Estado; a lo dispuesto en la Ley N°20.255 que establece Reforma Previsional; a lo dispuesto en la Ley 20.403 que Otorga un Reajuste de Remuneraciones a los Trabajadores del Sector Público, Concede Aguinaldos que señala, y Concede otros Beneficios que indica; a lo dispuesto en la Ley Nº19.628, sobre Protección a la Vida Privada; y atendidos los Principios de Colaboración y Gratuidad que informa las relaciones entre los distintos entes que conforman la Administración del Estado.

SEGUNDO: Objeto.

El presente Convenio tiene por objeto que **LA SUBSECRETARÍA** obtenga de **EL SERVICIO,** datos asociados al Registro Civil, bajo la modalidad de un servicio fuera de línea, estos es servicio batch, con la finalidad de contar con información de contacto de la población del país, para el levantamiento, implementación y ejecución de la VIII ola o Ronda de la Encuesta de Protección Social (EPS). Atendido lo anterior, **LA SUBSECRETARÍA** solicita la información nominada de contacto más actualizada que posea **EL SERVICIO** considerando que **LA SUBSECRETARÍA** es el organismo que tiene como función asesorar al Ministerio del Trabajo y Previsión Social en la elaboración de políticas y planes correspondientes al ámbito de la previsión social.

REGISTRO CIVIL E IDENTIFICACION
UNIDAD DE ATENCION DE INSTITUCIONES
CHILE

TERCERO: Datos y entrega de los datos.

Para cumplir con el objeto del presente convenio, **LA SUBSECRETARÍA** solicita la entrega de la siguiente información:

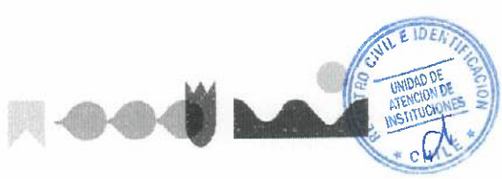
- RUN.
- Fecha de Nacimiento.
- Fecha de defunción, si registra.
- Sexo.
- Nombre completo.
- Domicilio (última actualización disponible).
- Comuna.
- Región.

EL SERVICIO proporcionará un archivo de texto con campos separados por slash o barra oblicua (/) con los siguientes datos de salida, cuya estructura será la siguiente:

Campo	Tipo (largo máx)	Observación
RUN	N(8)	RUN consultado
Dv	C(1)	Dígito verificador
Fecha de Nacimiento	N(8)	aaaammdd
Fecha de Defunción	N(8)	yyyymmdd;0 si no hay registro de defunción
Sexo	C(1)	M:masc, F:fem, I:indet, X:no bin, U:sin info
Apellido 1	C(75)	
Apellido 2	C(75)	
Nombres	C(75)	
Calle	C(75)	
Número	C(75)	
Letra	C(75)	
Resto	C(75)	
Comuna	C(75)	

Para estos efectos se entiende por último domicilio el que ha sido declarado a **EL SERVICIO** en cualquiera de las actuaciones o trámites que las personas puedan efectuar en sus dependencias.

Las partes dejan establecido, que el domicilio es un dato mutable que **EL SERVICIO** no se encuentra obligado por Ley a registrar, por lo cual, éste no puede dar fe de su vigencia y veracidad.



EL SERVICIO se compromete a entregar la información señalada en esta cláusula, sin perjuicio de las posibles modificaciones a que ésta pueda verse afectada.

CUARTO: Periodicidad y plazo de entrega de la información.

- Inicial: **EL SERVICIO** realizará la entrega de la información descrita en la cláusula anterior a **LA SUBSECRETARÍA**, relativa al universo de personas nacidas entre el 01 de julio de 1997 a 31 diciembre 2013, en un plazo de cinco (5) días hábiles.

- Bianual: **EL SERVICIO** realizará la entrega de la información descrita en la cláusula anterior a **LA SUBSECRETARÍA**, bianualmente, relativa al universo de personas nacidas entre el 01 de julio de 1997 hasta la nueva fecha de corte definida por **LA SUBSECRETARÍA** a informar a **EL SERVICIO**.

Cabe señalar que, para dar curso a lo anterior, **EL SERVICIO** requiere de un plazo para el desarrollo de la consulta necesaria de la extracción de la información de hasta diez (10) días hábiles, a partir del día siguiente de la total tramitación del presente convenio, informado por la Unidad de Atención de Instituciones a la Unidad de Inteligencia de Negocios de **EL SERVICIO**.

EL SERVICIO no será responsable por el incumplimiento de los plazos señalados, precedentemente, cuando ello obedezca a razones de caso fortuito, fuerza mayor o sobrecarga en el sistema computacional, debiendo informar de manera oportuna a **LA SUBSECRETARÍA.**

QUINTO: Operatoria en la entrega de datos.

La entrega de los archivos con la información requerida se realizará a través de descargas desde un servidor SFTP dispuesto por **EL SERVICIO** para tales efectos.

El acceso al servidor SFTP contará con credenciales de acceso institucional de **LA SUBSECRETARÍA**, con la finalidad de proteger y resguardar la integridad y confidencialidad de la información en él contenida, credenciales que serán informadas a través de correo electrónico por el Coordinador de **EL SERVICIO** al Coordinador de **LA SUBSECRETARÍA,** en un plazo de hasta tres (3) días hábiles, una vez que éstas sean generadas por parte de la Unidad de Infraestructura de **EL SERVICIO.**

EL SERVICIO se compromete a entregar la información de acuerdo al contenido de su base de datos al momento en que la consulta sea efectuada.

REGISTRO CIVIL E IDENTIFICACION
UNIDAD DE ATENCION DE INSTITUCIONES
CHILE

SEXTO: Control y Cumplimiento de las Obligaciones.

LA SUBSECRETARÍA, designará un Encargado de Protección de Datos, entre su personal, quien será el responsable de velar por el adecuado tratamiento y resguardo de la información, y generará un documento de seguridad de obligado cumplimiento en el que se recogerán las medidas de índole técnica y organizativa en el tratamiento de la información, acordes a la normativa vigente.

De conformidad a lo anterior, las personas que tengan acceso a la información que se entrega por el presente convenio, deberán conocer sus deberes de custodia y confidencialidad respecto a los datos o la documentación que tengan a su cargo, sus funciones y obligaciones, así como las normas de seguridad que afectan al desarrollo de las mismas, encontrándose claramente definidas y documentadas.

El cumplimiento de lo dispuesto en la presente cláusula podrá ser controlado por **EL SERVICIO**, a través de su coordinador, quién podrá exigir, entre otras acciones de control, la entrega de informes periódicos al Encargado de Protección de Datos de **LA SUBSECRETARÍA**, que digan relación con el tratamiento y resguardo de la información proporcionada a través del presente Convenio por **EL SERVICIO**.

SÉPTIMO: Limitaciones en el uso de la información.

LA SUBSECRETARÍA se obliga a utilizar la información proporcionada por **EL SERVICIO** o a la que tenga acceso con ocasión de la ejecución del presente convenio, sólo para los fines propios del presente convenio, manteniendo la confidencialidad correspondiente, en el marco de sus competencias legales, quedando prohibido un uso distinto al señalado. Asimismo, se obliga a limitar la divulgación de la información, materia de este convenio, sólo aquellos funcionarios o trabajadores, que estrictamente tengan la obligación de conocerla evitando el acceso a terceros no autorizados, debiendo adoptar medidas oportunas para garantizar que sus funcionarios y/o trabajadores mantengan dicha obligación de confidencialidad, incluyendo, de ser pertinente las respectivas cláusulas de confidencialidad en los contratos con sus funcionarios y/o trabajadores.

EL SERVICIO quedará liberado de toda responsabilidad por el uso indebido que **LA SUBSECRETARÍA** pueda dar a la información, reservándose el derecho a ejercer todas las acciones legales tendientes a demandar el reembolso de las sumas a las que eventualmente sea obligado a pagar como consecuencia de lo anterior, además de la indemnización de los perjuicios que se hubieren ocasionado.

REGISTRO CIVIL E IDENTIFICACIÓN UNIDAD DE ATENCIÓN DE INSTITUCIONES CHILE

LA SUBSECRETARÍA deberá instruir por escrito, de acuerdo a sus procedimientos formales internos, a cualquier funcionario que tenga acceso a la información, e incluir, de ser pertinente las respectivas cláusulas de confidencialidad en sus contratos, respecto a la imposibilidad absoluta de copiar total o parcialmente, como asimismo, revelar, publicar, difundir, vender, ceder, reproducir, interferir, interceptar, alterar, modificar, dañar, inutilizar, destruir, en todo o parte, dicha información, ya sea durante la vigencia del convenio como después de su término. Conforme a lo anterior, el/la Coordinador/a de **LA SUBSECRETARÍA** deberá enviar copia de dicha instrucción y/o de los respectivos contratos a el/la Coordinador/a de **EL SERVICIO**.

En consecuencia y especialmente, **LA SUBSECRETARÍA** se obliga a:

1. No hacer ningún uso de la información, antecedentes o base de datos diferente del previsto en el presente convenio, ya sea por sí misma o a través de sus filiales o terceros en general.
2. No transferir, ceder o transmitir a cualquier título, gratuito u oneroso, la información, antecedentes o base de datos generados, en virtud del convenio.
3. No transmitir o divulgar a terceros la información, antecedentes o bases de datos por ninguna otra vía o procedimiento.
4. No efectuar copia alguna, por ningún medio, ni bajo ningún concepto, de la información facilitada por **EL SERVICIO** para la realización del objeto del convenio.
5. Custodiar la información recibida a fin de que se garantice la protección adecuada de la misma y de su contenido, para evitar que personas no autorizadas o ajenas a la misma, puedan hacer uso indebido de ella.

Por consiguiente, **LA SUBSECRETARÍA** deberá velar por el cumplimento de la Ley N°19.628 Sobre Protección de la Vida Privada y garantizar que durante toda la vigencia del presente convenio no se infrinja de manera alguna cualquier normativa relacionada con el tratamiento de datos personales.

Cualquier incumplimiento de las obligaciones expresadas precedentemente por parte de **LA SUBSECRETARÍA** dará derecho a **EL SERVICIO** para poner término anticipado al presente convenio.

OCTAVO: Control de las actividades y las limitaciones de responsabilidad.

Para el acceso a la información, **LA SUBSECRETARÍA** debe disponer de mecanismos que le permitan identificar y autenticar de forma inequívoca y personalizada a los usuarios del sistema, y si la autenticación está basada en cuentas electrónicas, código o contraseñas asociadas a claves de acceso, éstas últimas caducarán periódicamente.

Cualquier uso de los datos que no se ajuste a lo dispuesto en la presente cláusula, será de responsabilidad exclusiva de **LA SUBSECRETARÍA**, frente a terceros y frente a **EL SERVICIO**, ante el que responderá por los daños y perjuicios que le hubiere podido causar, siendo considerado también responsable del tratamiento a estos efectos.

NOVENO: Normas y estándares internacionales para el procesamiento de los datos.

Las partes que suscriben el presente convenio, se obligan a cumplir con la normativa vigente en materia de protección de la vida privada y, en particular, con las normas y estándares internacionales para el procesamiento de los datos, sometiéndose tanto **EL SERVICIO** como **LA SUBSECRETARÍA**, a la normativa general de carácter internacional en materia de protección de datos personales y, en lo que resulte aplicable, al Reglamento General de Protección de Datos de la Unión Europea (RGPD).

Lo anterior, contempla un mínimo imperativo y tiene solo un carácter declarativo tanto por parte de **EL SERVICIO** como **LA SUBSECRETARÍA**.

DÉCIMO: Destrucción o devolución de información.

LA SUBSECRETARÍA se obliga a guardar el debido resguardo de la información, por lo tanto, los datos deben procesarse y, posteriormente, usarse o comunicarse a otras personas o entidades, solo para los fines establecidos en el presente convenio y no deben almacenarse más tiempo del que dure la vigencia del mismo.

Por lo tanto, una vez terminado el convenio, **LA SUBSECRETARÍA** se compromete a destruir los datos de carácter personal a los que accede a través de servicios en línea o fuera de línea, según corresponde, y si procede, los soportes donde conste esta información, dentro de los quince (15) días hábiles siguientes, una vez terminada la vigencia del presente convenio.

Esta destrucción consiste en la eliminación total de los datos existentes en los equipos informáticos utilizados y del total de la información a la que haya accedido **LA SUBSECRETARÍA**, en virtud del presente instrumento, cualquiera sea el soporte en que se contenga. Una vez destruidos, **LA SUBSECRETARÍA**, debe certificar su destrucción por escrito y el responsable del tratamiento de los datos de **LA SUBSECRETARÍA** debe hacer entrega del certificado que acredite tal destrucción al Coordinador designado en la cláusula Vigésimo Coordinadores/as de **EL SERVICIO**.

REGISTRO CIVIL E IDENTIFICACIÓN UNIDAD DE ATENCIÓN DE INSTITUCIONES CHILE

UNDÉCIMO: Propiedad y Exclusividad de los Sistemas de Información.

Para los efectos del presente convenio, se considerará propiedad de **EL SERVICIO** sin limitación alguna, los registros, diseños de hardware, redes y software, diagramas de flujo de programas y sistemas, estructuras de archivos, listados de código fuente u objeto, programas de computación, arquitectura de hardware, documentación y otros informes de su propiedad o proporcionados por éste, relacionados con la materia, todo lo cual, además, constituye información confidencial.

DUODÉCIMO: Gratuidad.

Los servicios que se prestan en virtud del presente convenio son gratuitos.

DÉCIMO TERCERO: Operatividad.

Las partes acuerdan que será responsabilidad de **LA SUBSECRETARÍA,** y a su costo, la implementación, mantención y reparación del mecanismo que permita hacer operable la entrega de la información de que da cuenta el presente convenio.

DÉCIMO CUARTO: Mantención, readecuación o interrupción.

Toda mantención, readecuación o interrupción de la operación del sistema, programada o no, deberá ser comunicada oportunamente, por parte de el/la Coordinador/a de **EL SERVICIO** mediante correo electrónico a el/la Coordinador/a de **LA SUBSECRETARÍA**.

EL SERVICIO quedará exento de toda responsabilidad por cualquier interrupción sea planificada o imprevista; o por la suspensión de la operación del sistema, que tengan su origen en labores de mantención o readecuación; o, caso fortuito o fuerza mayor

DÉCIMO QUINTO: Asistencia y Soporte Técnico.

La Unidad de Atención de Instituciones de **EL SERVICIO** proveerá y/o gestionará la correspondiente asistencia que requiera **LA SUBSECRETARÍA,** a propósito de la implementación del presente convenio, a través del correo electrónico convenios@registrocivil.gob.cl, de lunes a viernes entre las 09:00 a las 18:00 horas.

El/la Coordinador/a de **EL SERVICIO** informará anualmente a el/la Coordinador/a de **LA SUBSECRETARÍA,** los teléfonos de contacto para efectos de fortalecer la comunicación antes señalada.

REGISTRO CIVIL E IDENTIFICACIÓN UNIDAD DE ATENCIÓN DE INSTITUCIONES CHILE

DÉCIMO SEXTO: Daños y perjuicios.

EL SERVICIO quedará liberado de toda responsabilidad por los daños directos e indirectos, perjuicio previstos e imprevistos que pueda experimentar **LA SUBSECRETARÍA** como consecuencia directa de la información proporcionada, y que no sean imputables a **EL SERVICIO**.

Asimismo, **EL SERVICIO** no responderá por omisiones o errores en la información entregada, que no le sean imputables, considerando que los datos contenidos en su base de datos se encuentran asociados a los documentos fundantes correspondientes y cuya función es netamente registral.

DÉCIMO SÉPTIMO: Uso publicitario.

Todo uso publicitario que **LA SUBSECRETARÍA** quisiera hacer respecto de la transferencia de datos objeto del presente convenio, ya sea a través de prensa escrita, televisión, radio, internet u otros medios exteriores, deberá contar previamente con la autorización por escrito del Director Nacional de **EL SERVICIO**, evento en el cual **LA SUBSECRETARÍA** deberá informar los fines, el medio de difusión y el destinatario.

DÉCIMO OCTAVO: Vigencia y Duración.

El presente convenio entrará en vigencia a partir de la fecha de la total tramitación del acto administrativo que lo apruebe, y tendrá un plazo de duración de un (1) año, el que se renovará automáticamente por períodos iguales y sucesivos, por un máximo de (4) períodos, salvo que alguna de las partes manifieste a la otra su voluntad de poner término al convenio a través de un aviso, dirigido al Subsecretario de **LA SUBSECRETARÍA** o al Director Nacional de **EL SERVICIO**, según sea el caso.

Dicha comunicación, deberá ser notificada mediante Carta u Oficio, según correspondiere, con a lo menos treinta (30) días hábiles de anticipación a la fecha de vencimiento del plazo pactado precedentemente o de cualquiera de sus renovaciones.

DÉCIMO NOVENO: Término anticipado.

EL SERVICIO podrá poner término inmediato y en forma anticipada a la fecha de vencimiento o renovación del presente convenio, en los siguientes casos:

1. Que **LA SUBSECRETARÍA** no mantenga la reserva de la información considerada confidencial en los términos contemplados en este convenio.
2. Que el servicio permanezca interrumpido y sin uso conforme a la periodicidad que se indica en la cláusula CUARTO.

3. Que, en general, no se cumpla con alguna de las condiciones u obligaciones estipuladas en el presente convenio.
4. Por exigirlo el interés público o la seguridad nacional.
5. Por mutuo acuerdo entre las partes.
6. Que se verifique la existencia de leyes, decretos, reglamentos, sentencias judiciales o un nuevo procedimiento interno establecido por **EL SERVICIO** que regulen todo o algunas de las materias que por el presente convenio se establecen y que, en definitiva, limiten, restrinjan o prohíban la correcta ejecución de lo pactado en sus cláusulas, no permitan su ejecución o vuelvan innecesario o no operativo la prestación de servicios que por este convenio se regula.

VIGÉSIMO: Coordinadores.

Para los efectos de la correcta ejecución de cada una de las actividades y demás condiciones estipuladas en el presente convenio, así como todas las que sean establecidas en los instrumentos posteriores el objeto de velar por el fiel cumplimiento del presente convenio, cada una de las partes designará un coordinador:

- Por **EL SERVICIO**:
  La Jefa de la Unidad de Atención de Instituciones de **EL SERVICIO** por doña Andrea Muñoz Contreras, correo electrónico convenios@registrocivil.gob.cl, fono (56-2) 26114187, o quien la subrogue en el cargo.

- Por **LA SUBSECRETARÍA**:
  El Jefe de la Unidad de Observatorio Previsional de **LA SUBSECRETARÍA**, don Carlos Osorio Muñoz, correo electrónico carlos.osorio@previsionsocial.gob.cl, fono (56-2) 28279819, o quien la subrogue en el cargo.

En el evento de modificarse la designación de las coordinadoras, se deberá dar aviso a la otra parte por medio de correo electrónico, a más tardar dentro de los cinco (5) días siguientes a la fecha en que el cambio se produzca.

VIGÉSIMO PRIMERO: Copias.

Se deja constancia que el presente convenio se firma en dos (2) ejemplares de igual tenor y fecha, quedando uno en poder de cada parte.

VIGÉSIMO SEGUNDO: Anexos.

Las partes acuerdan que en el evento de ser necesario suscribir algún Anexo, éste se entenderá que forma parte integrante del convenio, lo que deberá ser aprobado mediante

Resolución del Subsecretario de **LA SUBSECRETARÍA** y del Director Nacional de **EL SERVICIO.**

VIGÉSIMO TERCERO: Solución de conflictos.

Para todos los efectos legales derivados del presente convenio, las partes fijan su domicilio en la comuna de Santiago y se someten a la jurisdicción de los Tribunales Ordinarios de Justicia.

VIGÉSIMO CUARTO: Personerías.

La personería de don Christian Larraín Pizarro, para actuar a nombre y en representación de **LA SUBSECRETARÍA**, consta en Decreto Supremo N°14 de fecha 11 de marzo de 2022, del Ministerio del Trabajo y Previsión Social que nombra al Subsecretario de Previsión Social.

La personería de don Omar Morales Márquez para actuar a nombre y en representación de **EL SERVICIO** consta en Decreto Supremo N°140, de 14 de diciembre de 2022, del Ministerio de Justicia y Derechos Humanos, que nombra al Director Nacional del Servicio de Registro Civil e Identificación, tomado de razón por la Contraloría General de la República, con fecha 11 de enero de 2023

CHRISTIAN LARRAÍN PIZARRO
SUBSECRETARIO DE PREVISIÓN SOCIAL
SUBSECRETARÍA DE
PREVISIÓN SOCIAL

OMAR MORALES MÁRQUEZ
DIRECTOR NACIONAL
SERVICIO DE REGISTRO CIVIL E
IDENTIFICACIÓN

RLLL/ DTB/ AMC

POLÍTICA DE CONVENIOS ASOCIADOS A LA PRESTACIÓN DE SERVICIOS DE VERIFICACIÓN O TRANSFERENCIA DE INFORMACIÓN CON INSTITUCIONES

ELABORADO POR	REVISADO POR	APROBADO POR
Andrea Muñoz Contreras Jefa Unidad de Atención de Instituciones	Sergio Mierzejewski Lafferte Subdirector de Estudios y Desarrollo	Jorge Alvarez Vásquez Director Nacional

V°B° Ingrid Reyes Constant – Subdirectora Jurídica

V°B° Gonzalo Navarrete Parra – Jefe de Riesgo Tecnológico y Seguridad TI

Control de Cambios

Nº Versión	Fecha	Motivo de la revisión	Páginas elaboradas o modificadas
0 (cero)	31/10/2012	Elaboración de acuerdo a los lineamientos del Sistema de Seguridad de la Información (SSI) y los requisitos de las normas NCh-ISO 27001:2013,	Todas.
1 (uno)	24/08/2015	Se ajusta el documento en los Principios de la Política.	Todas.
2 (dos)	20/11/2017	Se revisa número de versión de política. Se valida el contenido de la política y se actualizan los contenidos.	Todas.
3 (tres)	26/04/2018	Se revisa número de versión de política. Se valida el contenido de la política y se actualizan los contenidos.	Todas.
4 (cuatro)	31/07/2019	Se revisa número de versión de política. Se valida el contenido de la política y se actualizan los contenidos.	Todas.

- Jefe/a Unidad de Atención de Instituciones:
  - Revisar y aprobar la presente política.
  - Velar por el cumplimiento de la presente política.
  - Coordinar el proceso de revisión anual de la presente política.
  - Realizar modificaciones a la presente política, de ser pertinente.
  - Difusión de la política

- Funcionarios (as)del SRCeI:
  - Velar por el buen uso de la presente política.
  - Reportar errores, deterioros y problemas de seguridad a la Subdirección de Estudios y Desarrollo.

- Terceros externos contratados que requieran para el desarrollo de sus funciones el uso de la Política:
  - Velar por el buen uso de la presente política.
  - Reportar errores, deterioros y problemas de seguridad a la Subdirección de Estudios y Desarrollo.

IV. DEFINICIONES

La presente política forma parte de la documentación del Sistema de Seguridad de la Información del SRCeI y está orientada a formular las directrices generales que permitan minimizar el impacto de las amenazas y riesgos que pudiesen estar presentes, en materias de acuerdos sobre la verificación o transferencia de información, así como también, respecto de las limitaciones en el uso de la información.

Conforme a lo anterior, el SRCeI se compromete a gestionar la suscripción de distintos convenios de colaboración y/o prestación de servicios relacionados con la verificación o transferencia de información, con Instituciones Públicas y/o Privadas, conforme a sus condiciones técnicas, operativas y legales, bajo los siguientes lineamientos generales:

1. Velar por la protección de los datos personales, en la prestación de servicios de verificación o trasferencia de información en los convenios suscritos con distintas Instituciones Públicas y/o Privadas, en conformidad a lo dispuesto por la Ley N°19.628 sobre Protección a la Vida Privada.

2. Mejorar los niveles de satisfacción de los usuarios/as, respecto de la cobertura, acceso, oportunidad y calidad en la generación y entrega de los distintos productos y servicios, mediante la descentralización en la prestación de servicios de información por medio de la suscripción de convenios con distintas Instituciones.

3. Fortalecer el Rol del SRCeI dentro de la Sociedad.

4. Fomentar el uso de la atención virtual, a través del desarrollo de nuevos servicios no presenciales.

I. OBJETIVO

La presente política tiene por objetivo formular las directrices generales que permitan minimizar el impacto de las amenazas y riesgos que pudiesen estar presentes, en materias de acuerdos sobre la verificación o transferencia de información, así como también, respecto de las limitaciones en el uso de la información.

Lo anterior, a través de una gestión descentralizada mediante alianzas estratégicas que apunten a facilitar y simplificar los trámites que los/las ciudadanos/as efectúan en el SRCeI o en otras Instituciones Públicas y/o Privadas que mantengan convenio suscrito y vigente con el SRCeI, con el objeto de contribuir al nivel de satisfacción de los/as usuarios/as, así como también, en el fortalecimiento de la atención virtual.

II. ALCANCE

La presente política orienta su acción hacia toda verificación o transferencia de información desde el SRCeI a las distintas Instituciones Públicas y/o Privadas.

El presente documento debe ser cumplido por todos los funcionarios de planta y a contrata del SRCeI, así como también, de aquellos que se encuentren en calidad se suplente o reemplazo; al personal contratado a honorarios y a los terceros (incluyendo contratistas) que interactúen de manera habitual u ocasional con la Institución.

Esta política contempla los siguientes controles definidos en la norma NCh-ISO 27002-2013 vigente: 13.2.2. Acuerdos sobre la transferencia de información.

III. ROLES Y RESPONSABILIDADES

- Director/a Nacional:
  - Aprobar y difundir la presente política al interior del SRCeI.
  - Proveer los recursos necesarios para la implementación de la presente política.

- Jefe de Riesgo Tecnológico y Seguridad TI:
  - Informar sobre aquellas modificaciones que sean necesarias incorporar a la presente política.
  - Sugerir las modificaciones que sean necesarias de considerar, en la revisión anual de la presente política.
  - Visar la presente política.

- Subdirector de Estudios y Desarrollo:
  - Revisar y aprobar la presente política.
  - Proveer los recursos necesarios para la implementación de la presente política.
  - Velar por el cumplimiento de la presente política.

- Subdirector Jurídico:
  - Revisar y visar la presente política.

5. Generar alianzas estratégicas con otros organismos e instituciones, creando sinergias que permitan mejorar la entrega de los servicios a los usuarios y usuarias.

6. Mejorar continuamente la seguridad y disponibilidad de nuestros datos a través de la incorporación permanente de tecnologías de la información.

7. Incorporar enfoque de género y no discriminación, ya sea desde la redacción de los convenios que se suscriben con distintas Instituciones, así como también, a incentivar a éstas a contemplar e incorporar la perspectiva de género en las distintas etapas del ciclo de vida de las políticas públicas que puedan generar, mediante el acceso a servicios de información que el SRCel les pueda proporcionar.

Para el logro de estos objetivos, la Política de Convenios asociada a la prestación de servicios de verificación o transferencia de información con Instituciones, se sustentará en los siguientes lineamientos específicos:

1. Mantener y garantizar la confidencialidad, integridad y disponibilidad de los activos de información relevantes para el SRCel, de acuerdo con la Política de Seguridad de la Información.

2. Mantener y garantizar la confidencialidad de todos los antecedentes que se definan en los convenios suscritos, no pudiendo hacer uso de éstos para fines ajenos al mismo.

3. Asegurar que la información transferida esté protegida respecto de la imposibilidad absoluta de copiarla, total o parcialmente, revelar, publicar, difundir, vender, ceder, copiar, reproducir, interferir, interceptar, alterar, modificar, dañar, inutilizar y destruir.

4. Prohibir el traspaso de la información a terceros no autorizados que se entrega mediante la suscripción de convenios a las Instituciones Públicas y/o Privadas, así como de la información para su acceso.

5. Garantizar el correcto uso de la información únicamente para cumplimiento de los fines propios que se establecen en el objeto de los convenios suscritos, en conformidad a las competencias legales en el caso de Instituciones Públicas y para el caso de las Instituciones Privadas que digan directa relación con su giro.

6. Mantener una cartera actualizada de los servicios de verificación o transferencia de información a proveer a las Instituciones Públicas y/o Privadas, de tal forma, de contribuir al nivel de satisfacción de los usuarios/as.

7. Incentivar el uso de la tecnología en los procesos operativos de los convenios suscritos.

8. Reservarse la posibilidad de coordinar la supervisión, control y auditorías a las Instituciones Públicas y/o Privadas que cuenten con Convenios suscritos, en el marco del objeto del mismo

V. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

La presente política será evaluada y revisada al menos una (1) vez al año por el responsable de su elaboración o cuando el SRCel así lo requiera, con la finalidad de asegurar su continuidad e idoneidad, considerando cambios externos o internos que puedan afectarla.

Una vez que el documento entre en vigencia, el responsable de su elaboración deberá realizar las acciones indicadas en el apartado Difusión de este documento.

VI. DIFUSIÓN

La presente política deberá ser difundida a los funcionarios de planta y a contrata del SRCel, así como también, de aquellos que se encuentren en calidad se suplente o reemplazo, al personal contratado a honorarios y a los terceros (incluyendo contratistas), que interactúen de manera habitual u ocasional con la Institución.
Para estos efectos, el documento estará disponible y publicado en el sitio web del Sistema de Gestión Integral de Calidad del SRCel, específicamente, en la Documentación del Proceso de la Subdirección de Estudios y Desarrollo, cuya URL es la siguiente http://calidad.srcei.cl/qsm/

POLÍTICA CONTROLES CRIPTOGRÁFICOS

ELABORADO POR	REVISADO POR	APROBADO POR
María Cecilia Ríos Suazo Encargada de Seguridad de la Información	Edward Araya Astudillo Jefe Unidad de Gestión Estratégica (S)	Jorge Núñez Silva Director Nacional (S)

V°B° Rodrigo Vidal Kasija, Subdirector de Estudios y Desarrollo

V°B° Mónica Huerta Valderrama, Subdirectora Jurídica (S)

Contenido

REVISIONES

N°	Fecha	Motivo de la revisión	Páginas elaboradas o modificadas
01 (Uno)	30/11/2016	Elaboración Inicial, de acuerdo a los lineamientos del Sistema de Seguridad de la Información (SSI) y los requisitos específicos de los controles: A.10.1.1 – Controles criptográficos, A.10.1.2 – Administración de claves (llaves), A.18.1.5 – Regulación de controles criptográficos de la norma NCh27001:2013 Anexo A y NCh 27002:2013.	Todas
02 (Dos)	23/07/2019	Modifica orden del contenido. Modifica ítems V y VI.	Página 03 Página 04
03 (Tres)	19/03/2021	Revisión y actualización. Incorpora Norma NCh-ISO 27.701:2020	Todas
04 (Cuatro)	15/09/2022	Incorpora recomendaciones contenidas en el documento Informe con Resultados "Revisión y Medidas Aplicadas para Superar los Hallazgos" Medida 7.1.7, del Plan Visa Waiver liderado por Subdirección de Estudios y Desarrollo. Actualiza formato del documento.	Todas

1. DECLARACIÓN INSTITUCIONAL

El Servicio de Registro Civil e Identificación (en adelante el SERVICIO), se ha comprometido en 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, desarrolla un trabajo paulatino de implementación del Sistema de Seguridad y Privacidad de la Información (en adelante, SGSPI) basado en las Normas Chilenas NCh ISO 27.001:2013, NCH ISO 27.002:2013 y NCh ISO 27.701:2020.

2. INTRODUCCIÓN

Habitualmente la información es transmitida a través del correo electrónico, transacciones en línea, unidades USB, etc. Además, puede encontrarse almacenada fuera de las dependencias del SERVICIO, en servidores provistos por proveedores externos.
Por otra parte, la información a cargo de la institución puede ser pública o reservada, y la divulgación a personas o instituciones que no tienen la facultad para conocerla puede implicar incumplimientos a la normativa legal.
Dado esto, es necesario establecer controles criptográficos que permitan proteger la información durante su transmisión o transporte.

3. OBJETIVO

El objetivo de la presente política es definir reglas para el uso de controles y llaves criptográficas para proteger la confidencialidad, integridad, autenticidad e inviolabilidad de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante, en atención a los resultados de la evaluación de riesgos.

4. ALCANCE

La presente política aplica a todos los funcionarios y funcionarias de planta, contrata, honorarios, terceros externos contratados que prestan sus servicios al SERVICIO y que tengan acceso a información, en especial a información personal identificable (IPI) y sistemas que forman parte del SGSPI.

5. REFERENCIAS

- Ley N°19.799 - Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- 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.
- Decreto N°1 de 11-06-2015 del Ministerio Secretaría General de la Presidencia - Aprueba norma técnica sobre sistemas y sitios web de los Órganos de la Administración del Estado.
- Política de Seguridad y Privacidad de la Información del SERVICIO.
- Política de Clasificación y Manejo de Activos de Información.
- Norma NCh N°27001:2013 Anexo A, controles: A.10.1.1 Política sobre el uso de controles criptográficos, A.10.1.2 Gestión de claves, A.18.1.5 Regulación de los controles criptográficos.
- Norma NCh N°27002:2013, controles: 10.1.1 Políticas sobre el uso de controles criptográficos, 10.1.2 Administración de claves, 18.1.5 Regulación de controles criptográficos.
- Norma NCh N°27701:2020, controles: 6.7.1.1 Política sobre el uso de controles criptográficos, 6.7.1.2 Gestión de claves, 6.15.1.5 Regulaciones de los controles criptográficos.

6. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Director(a) Nacional	Aprobar la presente política.
Comité Directivo de Seguridad de la Información	Requerir la actualización de esta política, para asegurar su continuidad e idoneidad, considerando cambios externos o internos que puedan afectarla.
Encargada(o) de Seguridad de la Información	(i) Programar actividades de difusión de esta política. (ii) Evaluar y revisar anualmente esta política.
Subdirector(a) de Estudios y Desarrollo	(i) Establecer los procedimientos adecuados y velar por la no divulgación, modificación y/o destrucción involuntaria de claves criptográficas. (ii) Mantener un inventario actualizado de sistemas, aplicativos, procesos y activos de información que se encuentren afectos a controles criptográficos.

ROL	RESPONSABILIDAD
	(iii) Incorporar esta política en la definición de los perfiles de cargo que corresponda y en el proceso de inducción de los/las nuevos/as funcionarios/as que se integren a su dependencia.
Jefe Unidad de Gestión Estratégica	Mantener la versión actualizada de la presente política en el sitio web de la intranet institucional (https://intranet.beta.srcei.cl/).
Jefe Departamento de Identificación	(i) Incorporar esta política en la definición de los perfiles de cargo que corresponda y en el proceso de inducción de los/las nuevos/as funcionarios/as que se integren a su dependencia.
Administradores/as de Contrato	(i) Cuidar que el contenido de los acuerdos o contratos con proveedores externos que consideren la utilización o prestación de servicios criptográficos, contengan cláusulas de confidencialidad de dichos servicios. (ii) Enviar copia de esta política a los proveedores cuyos servicios digan directa relación con la materia.
Todos los funcionarios(as)	Cumplir la presente política.

7. DEFINICIONES

TÉRMINO	DEFINICIÓN
Activo de Información	Son todos aquellos elementos, documentos, sistemas, base de datos, infraestructura o personas 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 aquellas que tienen el conocimiento de los procesos institucionales.

TÉRMINO	DEFINICIÓN
Comité Directivo de Seguridad de la Información	Es el equipo conformado por el cuerpo directivo del SERVICIO, responsable de la toma de decisiones en temas de seguridad y privacidad de la información.
Datos Personales	Aquellos datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
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.
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.
Funcionario(a)	Toda persona que tenga un vínculo contractual de trabajo con el SERVICIO, independiente de la calidad jurídica: Planta, Contrata, Honorario, Código del Trabajo. Además, la presente política alcanza también a aquellos terceros externos contratados, que presenten sus servicios al SERVICIO.
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.
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.
Sistema de Seguridad y Privacidad de la Información	Conjunto de políticas, procedimientos e instructivos adoptados por el SERVICIO, para gestionar tanto la seguridad de la información como la privacidad de los datos personales y sensibles de los usuarios(as) que se contienen en los registros que la institución tiene a su cargo y administra por mandato legal.

TÉRMINO	DEFINICIÓN
Tratamiento	Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.
Criptografía	La criptografía -del griego κρύπτος (kryptós), «secreto», y γραφή (graphé), «grafo» o «escritura», literalmente «escritura secreta»- se ha definido, tradicionalmente, como el ámbito de la criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. La aparición de la informática y el uso masivo de las comunicaciones digitales, han producido un número creciente de problemas de seguridad. Las transacciones que se realizan a través de la red pueden ser interceptadas y, por tanto, la seguridad de esta información debe garantizarse. Este desafío ha generalizado los objetivos de la criptografía para ser la parte de la criptología que se encarga del estudio de los algoritmos, protocolos (se les llama protocolos criptográficos), y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

8. DIRECTRICES

a) Se deben utilizar controles criptográficos con el fin de garantizar la seguridad de la información, en especial de la información personal identificable, sea que la misma se trate de datos personales o de datos sensibles.

b) Todos los algoritmos y soluciones que incluyan controles criptográficos deberán diseñarse y aplicarse conforme a la legislación vigente.

c) Cuando corresponda, los controles criptográficos cumplirán los tratados internacionales vigentes en materia de uso de este tipo de tecnología.

d) La calidad y pertinencia de los controles criptográficos dependerá del grado de sensibilidad de la información o comunicación involucrada.

e) Todo sistema, aplicación o sitio web proporcionado por el SERVICIO, que requiera el ingreso o empleo de información personal identificable por parte del usuario/a (sea que la misma se trate de datos personales o de datos sensibles), deberá utilizar controles criptográficos que garanticen la confidencialidad de la comunicación.

f) Todo medio móvil, extraíble o canal de comunicación que transporte información deberá emplear medidas de seguridad acorde a su criticidad.

g) Se deben definir los medios o canales de comunicación permitidos para el transporte o transferencia de información.

h) Las claves criptográficas de los sistemas informáticos de propiedad del SERVICIO serán administradas por la Subdirección de Estudios y Desarrollo, quien deberá:

   i. Establecer los procedimientos adecuados y velar por la no divulgación, modificación y/o destrucción involuntaria de claves criptográficas.
   ii. Mantener un inventario actualizado de sistemas, aplicativos, procesos y activos de información que se encuentren afectos a controles criptográficos.

i) El contenido de acuerdos o contratos con proveedores externos que consideren la utilización o prestación de servicios criptográficos, deben contener cláusulas de confidencialidad de dichos servicios.

j) El SERVICIO podrá utilizar sistemas de cifrado basado en certificados digitales para verificar la autenticidad o integridad de la información almacenada o transmitida. En el caso de aplicaciones con Firma Electrónica Avanzada, esta deberá dar cumplimiento a la Ley N°19.799 - Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma.

9. CUMPLIMIENTO

El incumplimiento de esta Política será sancionado conforme lo establecido en el Procedimiento "Sanciones por el Incumplimiento de las Políticas y Normativa asociada a la Seguridad de la Información".

10. DIFUSIÓN

El SERVICIO mantendrá a disposición de los funcionarios/as, y del personal externo que se desempeñe en él, la versión actualizada de la presente política en el sitio web de la intranet institucional (https://intranet.beta.srcei.cl/).

Sin perjuicio de lo anterior, la(el) Encargada(o) de Seguridad de la Información debe programar actividades de difusión de esta Política al interior del SERVICIO. Asimismo, los Administradores/as de Contrato deben enviar copia de esta Política a los proveedores cuyos servicios digan directa relación con la materia.

El Subdirector/a de Estudios y Desarrollo y el Jefe/a del Departamento de Identificación deben incorporar esta Política en la definición de los perfiles de cargo que corresponda y en el proceso de inducción de los/las nuevos/as funcionarios/as que se integren a sus respectivas dependencias.

11. VIGENCIA Y REVISIÓN

La presente política será evaluada y revisada, al menos una vez al año por el/la 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:

(i) Cambios legales y/o normativos que puedan afectar a la presente política,
(ii) Técnicas criptográficas disponibles,
(iii) Eventos de seguridad que afecten la Confidencialidad, Integridad, Disponibilidad o Privacidad de los activos de 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.

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES PARA LA TRANSFERENCIA O VERIFICACIÓN DE DATOS A TERCEROS

ELABORADO POR	REVISADO POR	APROBADO POR
Enrique Sepúlveda Rivas Subdirector de Estudios y Desarrollo(S)	Javier Espinoza Gajardo Jefe Unidad de Gestión Estratégica	Sergio Mierzejewski Lafferte Director Nacional Servicio de Registro Civil e Identificación (S)

V°B° Mónica Huerta Valderrama, Subdirectora Jurídica (S)

Índice

HISTORIAL DE VERSIONES

N° de Version	Fecha	Motivo de la revisión	Páginas elaboradas o modificadas
N°0 (cero)	19/04/2021	Elaboración inicial de la política a propósito de los requisitos establecidos en la norma NCh NCh-ISO/IEC 27001:2013 y NCh-ISO/IEC 27701:2020.	Todas

1. DECLARACIÓN INSTITUCIONAL.

El Servicio de Registro Civil e Identificación (en adelante el SERVICIO o el SRCeI), dentro de sus Sistema de Gestión de Seguridad y Privacidad de la Información define como prioritario el proteger los datos personales contenidos en sus activos de información, conforme lo establecido en su Política de Seguridad y Privacidad de la Información y en las Normas Chilenas NCh ISO 27.001:2013 y NCh ISO 27.701:2020.

2. INTRODUCCIÓN

La información de identificación personal (IIP) 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, infracciones legales, incumplimiento regulatorio o contractual, vulneración de derechos de usuarios y usuarias, entre otros; por lo cual, es importante proteger adecuadamente dicha información.

3. OBJETIVOS

Los objetivos de la Política de Protección de Datos Personales para la Transferencia o Verificación de Datos a Terceros se encuentran alineados con el Sistema de Seguridad y Privacidad de la Información y corresponden a:

1) Cumplir con los principios de seguridad de la información y la privacidad de los datos.
2) Proteger todos los activos de la información de la institución y la información de identificación personal asociada a ellos.
3) Apoyar las garantías de la continuidad del negocio frente a incidentes de seguridad y privacidad de la información.

4. ALCANCE

La presente política tiene como alcance aquellos procesos de transferencia o verificación de datos a terceros que se realizan por medio de canales electrónicos, debiendo ser cumplida por todas las partes que se relacionen directa o indirectamente con aquél.

5. POLÍTICA

- Toda transferencia o verificación de datos personales a terceros que no esté expresamente regulada en una norma legal debe ser documentada y autorizada, a través de un acuerdo formal para tales fines, por quienes tengan las facultades para proceder en ese sentido.

- Todo acuerdo relativo a la transferencia o verificación de datos personales a terceros debe considerar el aspecto normativo y de riesgos de seguridad de la información previo a su suscripción, a fin de resguardar la integridad, disponibilidad, completitud y privacidad de dichos datos, esto implica la inclusión de cláusulas de acuerdos de confidencialidad, entre otros.

- La transferencia de datos personales, desde o hacia terceros, debe ser registrada, Los registros de transferencia se deben mantener respaldados en medios electrónicos (log de transacciones, planillas de cálculo, etc.) por un tiempo indeterminado.

- La divulgación de datos personales a terceras partes debe ser registrada, lo que incluye qué dato personal se reveló, a quién y en qué momento. Esto incluye divulgación que se derive de investigaciones legales o auditorías externas. En los registros, se deben incluir la fuente de la divulgación y la fuente de la autoridad para realizar la divulgación. Para estos efectos, se debe considerar que el SRCeI, en caso de ser requerido judicialmente, comunicará los datos personales de los(as) usuarios(as) que le sean solicitados.

- El usuario(a) puede en todo momento ejercer los derechos otorgados por la Ley N°19.628 sobre Protección de la Vida Privada y sus modificaciones posteriores, sin perjuicio de los límites que contempla la normativa legal al ejercicio de estos derechos, tales como la obligación de almacenamiento de los datos efectuada por mandato legal.

- Se establecerán procedimientos diseñados para:
  - Proteger la información transferida de la intercepción, la copia, la modificación, el ruteo incorrecto y la destrucción.
  - Proteger la información electrónica sensible comunicada en forma de elemento adjunto.

6. MARCO LEGAL, REGULATORIO Y NORMATIVO

- Política de Seguridad y Privacidad de la Información.
- Ley N°19.628 Protección de Datos Personales.
- Norma NCh-ISO/IEC 27001:2013; en específico controles contenidos y distribuidos en los siguientes dominios:
  A.13.2.1 Políticas y procedimientos sobre la transferencia de información.
- Norma NCh-ISO/IEC 27701:2020; en particular los siguientes controles:
  A.7.5 Intercambio, transferencia y eliminación de PII.
  B.8.5 Intercambio, transferencia y eliminación de PII.

7. ROLES Y RESPONSABILIDADES

Rol	Responsabilidad
Director(a) Nacional	• Proveer los medios para la implementación de esta Política. • Aprobar las versiones actualizadas de esta Política.
Encargado(a) de Seguridad y Privacidad de la Información (ESI)	• Difundir y sensibilizar respecto de la presente política.
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 para la transferencia o verificación de datos personales a terceros
Encargado(a) de Unidad de Atención a Instituciones	• Incorporar en los convenios de transferencia o verificación de datos a terceros, aquellas cláusulas que permitan proteger los datos personales contenidos en ellos.
Jefes de área	• Registrar toda transferencia de datos personales que se realice hacia terceros, que no forme parte de Convenios de transferencia o verificación de datos a terceros. Como, por ejemplo, respuestas de solicitudes de Ministerio Público, Contraloría General de la República, etc.

8. DIFUSIÓN

El SRCeI mantendrá a disposición de los funcionarios/as y personal que se desempeñe en él, la versión actualizada de la presente política 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/ y en el sitio web Intranet institucional (https://intranet.beta.srcei.cl/).

9. 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.

Sin perjuicio de lo anterior, esta política será siempre revisada cuando ocurra un evento relevante o un incidente de seguridad de la información.

10. SANCIONES POR INCUMPLIMIENTO

El incumplimiento de la presente Política y de los procedimientos o instructivos asociados, ya sea por parte del personal del SRCeI, independiente de su calidad estatutuaria, personal contratado a honorarios o personal perteneciente a empresas que presten servicios a la institución, 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.

En el caso de empresas que presten servicio a la institución, ya sea en forma permanente u ocasional, el Subdirector/a de Estudios y Desarrollo enviará una carta dirigida al Representante Legal de la empresa informando respecto de la infracción o incumplimiento observado.

En el caso de instituciones en convenio, las sanciones por incumplimiento se establecerán en el respectivo acuerdo.

11. 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.
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. 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. Se entiende equivalente a la Información de Identificación Personal o IIP.
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.

Término	Definición
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.
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.
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.
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.
Sistema de Seguridad y Privacidad de la Información	Sistema adoptado por el SRCel, 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 instituciones públicas o privadas que interactúan con el SRCel para efectos de la transferencia o verificación de datos personales contenidos en los registros a cargo del Servicio, en el contexto de norma legal expresa o convenio suscrito para tales efectos.
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 SRCel, independiente de la calidad jurídica: Planta, Contrata, Honorario, Código del Trabajo.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ELABORADO POR	REVISADO POR	APROBADO POR
María Cecilia Ríos Suazo Encargada de Seguridad de la Información	Enrique Eduardo Foos Lapostol Jefe Unidad de Gestión Estratégica	Director Nacional (s)

Jenny Lissette Nicolas Turrys — Subdirectora Jurídica

Rodrigo Alejandro Vidal Kasija — V°B° Rodrigo Vidal Kasija, Subdirector de Estudios y Desarrollo

ÍNDICE

HISTORIAL DE VERSIONES

N° de Versión	Fecha	Motivo de la revisión	Páginas elaboradas o modificadas
N°00 (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°01 (uno)	25/5/2016	Revisión a propósito de la actualización de la norma NCh NCh-ISO/IEC 27001:2013.	Todas
N°02 (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°03 (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°04 (cuatro)	16/09/2019	Revisión anual de la política según norma NCh ISO 27001:2013. Ajuste a estructura del documento.	Todas
N°05 (cinco)	03/11/2020	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
N°06 (seis)	03/03/2022	Revisión anual de la política según norma NCh NCh-ISO/IEC 27001:2013. Incorporación de observaciones efectuadas en Memorándum SJ N°1.653, del 29 de diciembre de 2021 y en correo electrónico de fecha 2/03/2022. Actualización normativa y de Subdirectora Jurídica y Subdirector de Estudios y Desarrollo, ambos nombrados el 3 de enero de 2022.	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 del Activo de Información que la institución considere relevante conservar. Para ello, desarrolla un trabajo paulatino de implementación del Sistema de Seguridad y Privacidad de la Información (en adelante, SGSI) basado en las Normas Chilenas NCh ISO 27.001:2013 y NCh ISO 27.701:2020, y en las Recomendaciones que a su respecto emanen del Consejo para la Transparencia, tendiente a homogeneizar los criterios de seguridad, con el objeto de preservar los activos de información de la Institución, en particular, respecto a su:

a) **Confidencialidad**: El SERVICIO cuidará 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. Por lo tanto, la información debe ser gestionada por los funcionarios(as) que la requieran única y exclusivamente para el desarrollo estricto de sus funciones.

b) **Integridad**: El SERVICIO cuidará 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. En definitiva, los activos de información no deben ser alterados o eliminados sin que esto sea debidamente autorizado, a fin de garantizar la precisión y validez de la información durante su procesamiento, así como evitar cualquier tipo de fraude que se pueda generar a partir de alteraciones o irregularidades.

c) **Disponibilidad:** El SERVICIO cuidará 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 de la institución, de modo tal que los(las) usuarios(as) autorizados(as) accedan a la información cuando se requiera en los distintos procesos institucionales. Esto debe considerar no solo la disponibilidad sino también la capacidad de procesamiento, permitiendo una recuperación rápida y completa ante algún

Dirección Nacional

evento que afecte la operatividad, o implique daños a las instalaciones o medios de almacenamiento.

d) **Privacidad:** El SERVICIO cuidará se apliquen los controles necesarios para proteger los activos de información a fin de resguardar adecuadamente la privacidad de los datos personales y sensibles de los usuarios(as) mantenidos en los registros a su cargo.

La gestión que emana de la presente Política de 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(as).

2. INTRODUCCIÓN

La información corresponde a un activo del SERVICIO, 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. La ocurrencia de aquellos riesgo y amenazas, puede provocar pérdidas materiales y económicas, daño en la imagen institucional y en la confianza de los usuarios(as), infracciones legales, incumplimiento regulatorio, vulneración de derechos de funcionarios(as) o de terceros, por lo cual, es importante proteger adecuadamente los activos de información por cuanto corresponde a un elemento relevante en el desarrollo de los procesos de provisión de productos o servicios estratégicos para el 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.

3. OBJETIVOS

Los objetivos de la Política de Seguridad y Privacidad de la Información, que se enmarcan dentro del Sistema de Seguridad y Privacidad de la Información del SERVICIO, corresponden a:

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

2) Proteger eficientemente los activos de información del SRCeI, asegurando su confidencialidad, integridad, disponibilidad y privacidad.

3) Cumplir con los principios de la protección de datos, esto es: Licitud, Calidad, Información, Seguridad y Confidencialidad.

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 del servicio, independiente de su calidad jurídica y de los proveedores de bienes y servicios adquiridos por esta entidad.

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

7) Establecer los requisitos y condiciones generales de protección y resguardo de seguridad y ciberseguridad a los que se encuentra sujeto el SRCeI, de acuerdo con las normas legales y reglamentarias pertinentes, así como los riesgos a que están expuestos sus activos de información y, los principios y objetivos internos para el resguardo de sus operaciones.

8) Definir una estructura y un marco de políticas, estándares y procedimientos en materia de seguridad de la información dentro del SRCeI.

9) Implementar, aplicar y ejecutar las medidas de ciberseguridad instruidas mediante el Instructivo Presidencial N°008, de 23 de octubre de 2018, el cual proporciona directrices en materia de ciberseguridad para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado.

4. ALCANCE

La presente política, debe ser cumplida por todas las personas, naturales o jurídicas que se relacionen directa o indirectamente con el SERVICIO 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; personal contratado a honorarios; y terceros (incluyendo contratistas y suscriptores de convenios) que interactúen de manera habitual u ocasional con la institución.

5. REFERENCIA NORMATIVA NCH/IEC.

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 y sensibles.

A partir de esta Política se definirán otras para regular materias específicas. A su vez, de las políticas se desarrollarán procedimientos e instrucciones 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 por la Ley N° 19.628, sobre Protección a la Vida Privada, y por la Resolución Exenta N°304, de 30 de noviembre de 2020, del Consejo para la Transparencia, que contiene las recomendaciones y buenas prácticas para la protección de datos personales por parte de la Administración del Estado.

Para efectos de establecer el sentido y alcance de un concepto contenido en esta Política, se consideran las definiciones contenidas en el artículo 2°, de la Ley N°19.628, ya señalada.

Los datos serán clasificados de la siguiente manera:

a) **Datos de carácter personal:** Se definen como aquellos antecedentes relativos a cualquier información concerniente a personas naturales, identificadas o identificables. El tratamiento de estos datos sólo puede efectuarse cuando una 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:** Se definen como aquellos antecedentes 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. En virtud de lo establecido en el Artículo 7°, inciso 2°, de la letra i) de la Ley N° 20.285, Sobre Acceso a la Información Pública, 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, tienen como característica que su consulta puede ser efectuada por cualquier persona, como ocurre, por ejemplo, con los contenidos de diarios y/o medios de comunicación social.

Por su parte, los datos personales de los(as) usuarios(as) que son recopilados a través de actuaciones, mediatizadas por diversos formularios y sistemas computacionales asociados entre sí, el SERVICIO los tiene disponibles a través de sus distintas plataformas de atención, constituidas por las oficinas presenciales, por la Oficina Internet, los módulos de trámites y servicios en línea del sitio web institucional (www.registrocivil.cl), por el portal Gobierno Transparente, los quioscos de autoatención y aplicaciones móviles.

La disponibilidad de los datos a través de los medios antes señalados, son entregados conforme las competencias y atribuciones, que por ley se han radicado en el SERVICIO, conforme lo dispone la Ley N° 19.477, Orgánica del Servicio de Registro Civil e Identificación.

Los datos personales de los usuarios(as) son recolectados, almacenados, usados y puestos en circulación conforme los cuerpos legales que correspondan a la materia, en particular, a lo dispuesto en la Ley N°19.628, Sobre Protección de la Vida Privada, y en la Resolución Exenta N°304, del Consejo para la Transparencia, que contiene las recomendaciones y buenas prácticas para la protección de datos personales por parte de la Administración del Estado.

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:** aquel 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 de aquellos.

b) **Registros no automatizados:** aquel 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 mayores requisitos, a sus datos personales.

El SERVICIO, atendido a que por mandato expreso de ley tiene a su cargo los registros y bancos de datos personales, es responsable respecto de las decisiones relacionadas con el tratamiento de dichos datos.

Conforme lo anterior, la protección de datos está basada en los siguientes principios, definidos en la Resolución Exenta N°304, del Consejo para la Transparencia, ya señalada, en el numeral 4. PRINCIPIOS ORIENTADORES DE LA PROTECCIÓN DE DATOS, a saber:

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. Deber 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 SERVICIO 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, que Aprueba la Ley Orgánica del Servicio de Registro Civil e Identificación.

6.2 Titular de los Datos Personales.

Los antecedentes de carácter personales se asocian a una persona natural denominada "titular". Esta persona tiene derecho a conocer:

a) Información de los bancos de datos de responsabilidad del SRCel, 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 administrativa o judicialmente.

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 SERVICIO como Responsable del Tratamiento de los Datos personales

El SERVICIO, como Responsable del Tratamiento de Datos Personales, 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 SRCel- 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 SRCel 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 SRCel 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 REGULATORIO GENERAL

El tratamiento de los datos de carácter personal en registros o bancos de datos, así como su obtención y administración por parte de este SERVICIO, se encuentra regulado por los siguientes cuerpos normativos:

a) **Ley N°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."

b) **Ley N°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.

c) **Ley N°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.

d) **Ley N° 20.285, Sobre Acceso a la Información Pública:** tiene por objeto regular el principio de transparencia de la función pública, el derecho de acceso a la información de los órganos de la Administración del Estado, los procedimientos para el ejercicio del derecho y para su amparo, y las excepciones a la publicidad de la información.

e) **Ley N°21.180, sobre Transformación Digital del Estado:** tiene por objeto iniciar la evolución digital de las instituciones estatales, modificando diversos cuerpos normativos, incorporando el soporte y la tramitación electrónica en los procedimientos administrativos del Estado y la gestión documental.

f) **Ley N°19.223, Ley de Delitos Informáticos:** que tipifica figuras penales relativas a la informática y tiene por finalidad proteger la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de esta 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)

g) **Decreto Supremo N°83, Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos:** Establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado.

h) **Resolución Exenta N°304, de 2020:** del Consejo para la Transparencia, que aprueba el texto refundido y actualizado de las Recomendaciones sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado.

i) **Instructivo Presidencial N°008, de 2018:** el cual imparte directrices en materia de ciberseguridad para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado.

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

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

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

La enumeración de normas aquí señaladas, debe entenderse como aquel acervo normativo básico que permite comprender el nuevo derecho fundamental a la protección de los datos personales, que implican mandamientos jurídicos, instrucciones y/o recomendaciones que aportan criterios jurídicos a este SERVICIO para el tratamiento de los señalados datos personales, acción que se encuentra inserta en el ámbito de sus competencias asignadas por ley.

8. ROLES Y RESPONSABILIDADES

El SERVICIO contará con una estructura funcional para administrar el Sistema de Seguridad y Privacidad de la Información (SSI) constituida por las siguientes instancias (Roles) a los cuales se les asignarán determinadas responsabilidades.

8.1. 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) Oficial de Seguridad TI (OSI)

f) Jefe(a) Unidad Control de Riesgos y Seguridad

g) Encargado(a) de Ciberseguridad

h) Encargados/as de Seguridad de la Información Regionales

i) Encargado del Tratamiento de Datos

j) Responsable del Tratamiento de Datos

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. • 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 SRCel 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(las) funcionarios(as) del SRCel.
Oficial de Seguridad TI (OSI)	• Prestar asesoría técnica especializada al ESI, al Subdirector(a) de Estudios y Desarrollo y al Director(a) Nacional en las materias relativas a riesgos y seguridad de los Sistemas Informáticos y Documentos Electrónicos.

Rol	Responsabilidad
Jefe Unidad Control de Riesgos y Seguridad	• Subrogar al o a la Encargada de Seguridad de la Información. • Establecer estrategias preventivas, correctivas y reductivas que deben emprenderse frente a los riesgos de seguridad detectados. • Definir y coordinar la implementación de planes de corto, mediano y largo plazo relativos a la seguridad de la información para asegurar la continuidad operativa del Servicio.
Encargado(a) de Ciberseguridad	• Gestionar la seguridad informática del Servicio y los riesgos asociados a la Ciberseguridad. • Asesorar al o a la Encargada de Seguridad de la Información en materias de riesgo y ciberseguridad.
Encargados(as) de Seguridad y Privacidad de la Información Regionales	• 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. • Informar a ESI, cualquier acto anómalo detectado sobre el tratamiento de los activos de información.
Encargado del Tratamiento de Datos	• Es la jefatura encargada de un Registro en particular, quien 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 o designación.

Además, será responsabilidad individual inexcusable de los funcionarios(as) de calidad jurídica: titular, contrata, suplencia y/o reemplazo, personal a honorarios y

Dirección Nacional

terceros contratados que prestan servicios, que tengan acceso a los activos de información del SRCel, 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 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.

El o la Encargada de Seguridad de la Información debe coordinar la revisión de esta Política y gestionar su aprobación final por parte de la Dirección Nacional del SRCel.

9. DEL USO DE RECURSOS INSTITUCIONALES

Los funcionarios(as), personal o terceros deben resguardar adecuadamente los activos de información a los cuales tienen acceso.

De esta manera, y sin perjuicio de lo que se disponga en específico respecto del almacenamiento y mantenimiento de activos de información por parte del SERVICIO, la utilización de equipamiento de procesamiento o almacenamiento de información, tales como notebooks, PC, teléfonos móviles, maletas de atención terreno, medios extraíbles, entre otros, así como aplicativos para los cuales cuentan con permisos de acceso, como por ejemplo el Sistema de Identificación, Sistema Monito, Sistema de Atención Ciudadana, Plataforma de Transparencia, etc., redes locales, redes inalámbricas (WiFi), VPN, Internet, Intranet y correo electrónico, deben ejecutarse sólo para el cumplimiento de las labores encomendadas y con apego estricto a las políticas, procedimientos e instrucciones de trabajo que correspondan.

10. DIFUSIÓN

El SRCel mantendrá a disposición de los funcionarios/as, y del personal externo que se desempeñe en él, la versión actualizada de la presente política en el sitio web del Sistema de Gestión Integral de Calidad del SRCel, específicamente, en la Documentación del Proceso de Seguridad de la Información, cuya URL es la siguiente http://calidad.srcei.cl/gsm/ y en la intranet (https://intranet.beta.srcei.cl/). Por otra parte, en el sitio web institucional, en la sección "Política de Seguridad y

Privacidad" se publicará, para conocimiento de la ciudadanía, la Declaración Institucional contenida en el presente documento.

Sin perjuicio de lo anterior, la(el) Encargada(o) de Seguridad de la Información debe programar actividades de difusión de esta Política al interior del SRCeI y coordinar con la Subdirección de Estudios y Desarrollo y Subdirección de Administración y Finanzas, el envío de este documento a las instituciones con convenio vigente y a los proveedores.

El Departamento de Gestión y Desarrollo de las Personas debe incorporar la aplicación de las políticas de seguridad de la información en el Plan de Capacitación Anual y en el proceso de inducción institucional, velando por la correcta entrega de dicha información a los nuevos funcionarios que se integren al Servicio.

11. VIGENCIA Y REVISIÓN

La presente política será evaluada y revisada, al menos, una vez al año por el o la Encargada 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 SERVICIO 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.

12. SANCIONES POR INCUMPLIMIENTO

Las sanciones ante el incumplimiento de la presente Política, así como la de cualquier otra política, procedimiento o instructivo, asociados al Sistema de Seguridad y Privacidad de la Información del SERVICIO, se encuentra regulada en el Procedimiento Sanciones por Incumplimiento de las Políticas y Normativa Asociada a la Seguridad de la Información, en el cual se desarrolla, pormenorizadamente, el procedimiento que se debe seguir para aplicar las sanciones disciplinarias y aquellas acciones tomadas en ejercicio del control jerárquico de las jefaturas, ante incumplimientos de las normas y procedimientos establecidos en materia de seguridad de la información del Servicio, por parte de los/las funcionarios(as) de planta y contrata, suplencia o reemplazo, personal a honorarios y terceros externos contratados, que prestan servicios y que tengan acceso a los activos de información de la Institución.

- **Sanciones que se pueden aplicar al determinarse la responsabilidad Administrativa de un funcionario por medio de un procedimiento disciplinario.**

En relación a este procedimiento, las sanciones que pueden aplicarse son de cuatro clases:

a) Censura

b) Multa

c) Suspensión del empleo desde treinta días a tres meses

d) Destitución

- **Sanciones para personal externo al SERVICIO**

En el caso que personal externo, se encuentre o no trabajando en dependencias del Servicio, pero que tenga alguna labor que desempeñar, ya sea constantemente o a modo parcial en la institución, y que incurra en cualquier falta a la política, normas o procedimientos de seguridad de la información aprobadas por el Servicio, 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, notificándole la falta cometida y solicitándole tomar las acciones correspondientes y que estime necesarias, sin perjuicio de lo establecido en las cláusulas del respectivo contrato o convenio.

13. DEFINICIONES

Término	Definición
Activo de Información	Son todos aquellos elementos, documentos, sistemas, base de datos, infraestructura o personas 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 aquellas 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	Expectativas que el SRCel tiene con respecto al cuidado que el(la) funcionario(a) debe emplear para con los activos de información que este les entrega para el desempeño de sus funciones.
Comité de Seguridad y Privacidad	Es el equipo conformado por funcionarios(as) de las áreas de la institución, responsable de la toma de decisiones en temas de seguridad y privacidad de la información. En el caso del SRCel, se cuenta con un Comité Directivo de Seguridad y Privacidad de la Información (CDS) y un Comité Operativo de Seguridad y Privacidad de la Información (COS).
Confidencialidad	Obligación legal de mantener reserva de la información del SRCel a la que se acceda y que será exigible a cualquier persona natural o jurídica que interactúe o se relacione con el SRCel 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 Sensible	Aquellos antecedentes 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

Término	Definición
	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.
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, 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, 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, debiendo ajustar su proceder 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.
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

Término	Definición
	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.
Política	Directriz u orientación general expresada formalmente por la Alta Dirección del Servicio.
Procedimiento	Sucesión cronológica de acciones concatenadas entre si, 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(la) funcionario(a) usuario(a) a cargo de la manipulación de datos personales, sea que efectúe dicha manipulación mediante procedimientos automatizados o no automatizados.
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 Servicio de Registro Civil e Identificación.
Riesgo	Es el 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	Una vez que opera el tratamiento de un riesgo, a pesar de un cuidadoso diseño e implementación, puede no producir los resultados esperados y generar consecuencias no previstas. Aquellas consecuencias se entienden como Riesgo Residual.
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.

Término	Definición
Sistema de Gestión en Privacidad de la Información (SGPI)	En el caso la gestión de la Seguridad de la Información, forma parte del Sistema de Seguridad y Privacidad de la Información del SERVICIO. El SGPI es el régimen en el que se integra la gestión eficaz de la privacidad incorporando requisitos adicionales para el procesamiento de datos personales. También forma parte del Sistema de Seguridad y Privacidad de la Información del SERVICIO.
Sistema de Seguridad y Privacidad de la Información	Conjunto de políticas, procedimientos e instructivos adoptados por el SRCel, para gestionar tanto la seguridad de la información como la privacidad de los datos personales de los usuarios(as) que se contienen en los registros que la institución tiene a su cargo y administra por mandato legal.
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 SRCel, 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.