Providencia
Vida Buena
Secretaría Municipal

PROVIDENCIA, 08 MAY 2026

EX.N° 757 **/ VISTOS:** Lo dispuesto por los artículos 5 letra d), 12 y 63 letra i) de la Ley N°18.695, Orgánica Constitucional de Municipalidades; y

CONSIDERANDO: 1.- El Convenio de Adhesión Conectividad y Prestación de Servicios de Información de Dirección de Tránsito, Juzgado de Policía Local e Inspección Municipal suscrito, con fecha 21 de abril de 2026, entre la **MUNICIPALIDAD DE PROVIDENCIA** y el **SERVICIO DE REGISTRO CIVIL E IDENTIFICACION.-**

2.-El Oficio SUBD AI ORD.: N°111/2026 de fecha 22 de abril de 2026, del Servicio de Registro Civil e Identificación, Ingreso Externo N°3829 de 28 de abril de 2026.-

3.- El Memorándum N°7.358 de 28 de abril de 2026 de la Dirección de Tránsito y Transporte Público. -

DECRETO:

1.- Ratifícase el Convenio de Adhesión Conectividad y Prestación de Servicios de Información de Dirección de Tránsito, Juzgado de Policía Local e Inspección Municipal suscrito, con fecha 21 de abril de 2026, entre la **MUNICIPALIDAD DE PROVIDENCIA** y el **SERVICIO DE REGISTRO CIVIL E IDENTIFICACION, RUT.N°61.002.000-3**, que tiene por finalidad que **LA MUNICIPALIDAD** obtenga los certificados e información en el **SERVICIO,** bajo la modalidad en línea, para los efectos de acceder a la emisión de los documentos electrónicos y consultas a la base de datos que se indican, los que serán utilizados dentro del marco de las competencias de la Municipalidad.-

2.- El texto del referido Convenio se adjunta al presente Decreto y será considerado parte integrante del mismo. -

Anótese, comuníquese y archívese. -

MUNICIPALIDAD DE PROVIDENCIA
SECRETARIO ABOGADO MUNICIPAL

MARIA RAQUEL DE LA MAZA QUIJADA
Secretario Abogado Municipal

JAIME BELLOLIO AVARIA
Alcalde

RBC/MRMQ/IMYJ/fhm. -
Distribución:
Interesada
Dirección de Tránsito y Transporte Público
Primer Juzgado de Policía Local
Segundo Juzgado de Policía Local
Tercer Juzgado de Policía Local
Dirección de Fiscalización
Dirección Jurídica
Dirección de Control
Archivo
Decreto en Trámite N° 1524 /

CONVENIO DE ADHESIÓN
CONECTIVIDAD Y PRESTACIÓN DE SERVICIOS DE INFORMACIÓN
DIRECCIÓN DE TRÁNSITO, JUZGADO DE POLICÍA LOCAL
E INSPECCIÓN MUNICIPAL
ENTRE
EL SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN Y
LA ILUSTRE MUNICIPALIDAD DE PROVIDENCIA

21 ABR 2025

En Santiago de Chile, a ....., entre 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 [redacted], ambos domiciliados en [redacted], comuna de [redacted], [redacted] de [redacted] y la Ilustre Municipalidad de Providencia, en adelante la MUNICIPALIDAD, RUT Nº69.070.300-9, representada por su Alcalde, don Jaime Bellolio Avaria, RUN N[redacted], ambos domiciliadas en Pedro de Valdivia N°963, Providencia, Región de Metropolitana, se ha acordado lo siguiente:

PRIMERA: Antecedentes Legales y de Hecho.

Antecedentes Legales:
El presente Convenio se suscribe de conformidad a lo dispuesto en el Decreto con Fuerza de Ley N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N°19.880, de 2003, del Ministerio Secretaría General de la Presidencia, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; la Ley N°19.477, de 1996, del Ministerio de Justicia, que Aprueba Ley Orgánica del Servicio de Registro Civil e Identificación; el Decreto Ley N°645, de 1925, del Ministerio de Justicia, sobre el Registro General de Condenas; el Decreto Nº64, de 1960, del Ministerio de Justicia, que Reglamenta la Eliminación de Prontuarios Penales, de Anotaciones, y el Otorgamiento de Certificados de Antecedentes; la Ley N°18.883, que Aprueba el Estatuto Administrativo para Funcionarios Municipales; en el Decreto N°307, de 1978, del Ministerio de Justicia, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N°15.231, Sobre Organización y Atribuciones de los Juzgados de Policía Local; la Ley N°18.287, de 1984, del Ministerio de Justicia, que Establece Procedimiento ante los Juzgados de Policía Local; el Decreto con Fuerza de Ley N°1, de 2009, del Ministerio de Transporte y Telecomunicaciones y Ministerio de Justicia, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley de Tránsito; el Decreto Nº22, de 2021, del Ministerio de Justicia y Derechos Humanos, que Aprueba Reglamento del Registro de Vehículos Motorizados y deroga Decreto Supremo N°1.111, de 1984, del Ministerio de Justicia; el Decreto Supremo Nº61, de

2008, del Ministerio de Justicia, que Aprueba Reglamento del Registro de Multas de Tránsito No Pagadas; el Decreto Supremo N°170, del año 1985, Reglamento para el otorgamiento de Licencias de Conductor, del Ministerio de Transportes y Telecomunicaciones; el Decreto Supremo N°97, del año 1984, Reglamento para obtener autorización de otorgar Licencias de Conductor, del Ministerio de Transportes y Telecomunicaciones; el Decreto Supremo N°23, del año 2000, que Fija especificaciones del documento Licencia de Conductor, del Ministerio de Transportes y Telecomunicaciones; la Ley Nº19.628, de 1999, del Ministerio Secretaría General de la Presidencia, sobre Protección de la Vida Privada; el Decreto Supremo N°140, del Ministerio de Justicia y Derechos Humanos, que Nombra al Director Nacional del Servicio de Registro Civil e Identificación, de 14 de diciembre de 2022; la Resolución N°36, que Fija Normas sobre Exención del Trámite de Toma de Razón, promulgada en fecha 19 de diciembre de 2024, y publicada el 23 de diciembre de 2024 y la Resolución N°8, de 12 de abril de 2025 que modifica y complementa Resolución N°36, ambas de la Contraloría General de la República; y atendidos los Principios de Colaboración y Gratuidad que informa las relaciones entre los distintos entes que conforman la Administración del Estado; en el Decreto Supremo N°69, de 2021, del Ministerio de Transportes y Telecomunicaciones, que aprueba la Implementación del Proyecto "Licencia Digital".

Antecedentes de Hecho.

Con fecha 13 de marzo de 2025, la Subsecretaría de Transportes y el Servicio de Registro Civil e Identificación suscribieron el Convenio de Colaboración y Conectividad en el Marco de la Implementación de la Licencia Digital a cargo de la Subsecretaría de Transportes, según consta en Resolución Exenta N°104 de fecha 17 de marzo de 2025 del **SERVICIO**.

Lo anterior, en el marco de la ejecución del proyecto "Licencia Digital", contemplado en el Decreto Supremo N°69, de 2021, del Ministerio de Transportes y Telecomunicaciones, busca entre otras acciones, permitir a las Municipalidades autorizadas para otorgar Licencias de Conductor, consultar los informes emitidos por el Registro Nacional de Conductores de Vehículos Motorizados, a que se hace mención en el artículo 14 y en el Título XVIII de la Ley de Tránsito.

En virtud de ello, nace el Sistema de Gestión de Licencias de Conducir (SGL), el que permitirá modernizar y hacer más seguro el proceso de otorgamiento de licencias, centralizando e interoperando la información que se envía desde las Direcciones de Tránsito hacia el Registro Nacional de Conductores de Vehículos Motorizados.

La citada Subsecretaria tiene la calidad de proveedor y administrador de dicha Plataforma Electrónica, el que permitirá otorgar los mecanismos tecnológicos a través de los cuáles las Municipalidades autorizadas para otorgar licencias de conducir, den cumplimiento a la obligación establecida en el artículo 214 de la Ley de Tránsito.

Es así como las Municipalidades, a través de los Departamentos de Tránsito y Transporte Público Municipal deberán remitir la información respecto al otorgamiento de una licencia de conductor, al Registro Nacional de Conductores de Vehículos Motorizados del **SERVICIO**.

Por lo antes expuesto y en particular para la emisión de determinados certificados, que se detallan en la cláusula siguiente, **LA MUNICIPALIDAD** podrá acceder a ellos, tanto a través del Sistema de Gestión de Licencias de Conducir (SGL) de Subsecretaría de Transportes como por medio del aplicativo Monito *Web* u otro que en el futuro determine **EL SERVICIO.**

Con fecha 25 de octubre de 2023, se suscribió el Convenio de Adhesión Conectividad y Prestación de Servicios de Información entre el Servicio de Registro Civil e Identificación y la Municipalidad de Providencia, según consta en la Resolución Exenta N°431, de fecha 30 de octubre de 2023 de **EL SERVICIO**.

Sin embargo, **LA MUNICIPALIDAD** requiere ampliar los puestos de trabajo utilizados, motivo por el cual, a través de la suscripción del presente convenio se regularizará aquello

SEGUNDA: Objeto.

El presente Convenio de Adhesión tiene por finalidad que **LA MUNICIPALIDAD** obtenga los certificados e información en el **SERVICIO**, bajo la modalidad en línea, para los efectos de acceder a la emisión de los documentos electrónicos y consultas a la base de datos que a continuación se indican y según así corresponda, los que serán utilizados dentro del marco de las competencias de **LA MUNICIPALIDAD**.

Por su parte y de acuerdo a lo señalado en la cláusula PRIMERO "Antecedentes de Hecho", **LA MUNICIPALIDAD** podrá emitir a través del Sistema de Gestión de Licencias de Conducir (SGL) los siguientes certificados del **SERVICIO**:

1. Certificado de Antecedentes Conductor de uso exclusivo para obtención o renovación de Licencias de conductor.
2. Certificado de Antecedentes Conductor de uso exclusivo Juzgados de Policía Local y Municipalidades.

Cabe señalar, que **LA MUNICIPALIDAD** podrá emitir los certificados antes indicados tanto a través del aplicativo Monito *Web* **EL SERVICIO** como por el citado Sistema de Gestión de Licencias de Conducir (SGL).

Por su parte, **EL SERVICIO** en el futuro podrá adoptar otros mecanismos de conectividad o sustitutos al citado aplicativo Monito *Web*, que resulten necesarios para asegurar la interoperabilidad, seguridad y operatividad del sistema, de conformidad con las disposiciones legales y técnicas aplicables.

TERCERA: Requisitos para la Conectividad.

La conexión de cada puesto de trabajo a la red corporativa del SERVICIO para el acceso al aplicativo Monito *Web* se realizará a través de Internet, debiendo **LA MUNICIPALIDAD** para tal efecto, cumplir las siguientes condiciones técnicas:

1. Una dirección IP única, la cual servirá para conectar múltiples puestos de trabajo.
2. Un PC con navegador Microsoft Edge con compatibilidad Internet Explorer con *Windows* versión 10 u 11 profesional, ya que sólo de esta forma el sistema funciona en forma óptima.
3. Impresora láser blanco negro o color, emulación HP PCL 5.0 ó 6.0, conexión USB 2.0, al menos 16 MB de memoria interna, al menos 20 páginas por minuto (ppm), impresión de primera hoja menor de 8,5 segundos, resolución de 600x600 dpi o superior, bandeja inferior para papel carta y oficio, bandeja multiuso carga manual. Compatible con Internet *Explorer, Edge* y *Google Chrome.*
4. *Framework* idealmente en su versión 4.0 o superior. Compatible *Framework* 2.0 o superior.

El papel y tóner para las impresoras, necesarios para la emisión a través del aplicativo Monito *Web* de los documentos electrónicos que se detallan en la cláusula CUARTO, serán de cargo de **LA MUNICIPALIDAD**.

Por otra parte, los requisitos de conectividad para el acceso al Sistema de Gestión de Licencias de Conducir (SGL) serán aquellos definidos e informados por la Subsecretaría de Transportes a **LA MUNICIPALIDAD**.

CUARTA: Acceso y Puestos de Trabajo.

LA MUNICIPALIDAD podrá acceder a la red y al aplicativo Monito *Web* del SERVICIO durante doce (12) horas al día, seis (6) días a la semana, a través de ciento cincuenta (150) puestos de trabajo, con un máximo de tres (3) cuentas de acceso para cada puesto de trabajo, con la finalidad de emitir los certificados electrónicos y acceder a la consulta a la base de datos, que se señalan en el presente convenio:

- Treinta (30) puestos de trabajo estarán ubicados en la Dirección de Tránsito Municipal, desde el cual sólo se podrá acceder a la emisión de los certificados electrónicos valorados que a continuación se detallan:

    1. Certificados de Antecedentes de Conductor, los que se utilizarán sólo para la obtención de duplicados de licencias de conducir extraviadas, o destruidas total o parcialmente, de acuerdo con lo establecido en el artículo 29 de la Ley N°18.290, de Tránsito.

2. Certificado de Antecedentes de Conductor, con el fin de obtener o renovar la licencia de conducir, el cual, una vez solicitado, sólo se emitirá para los fines descritos, debiendo quedar registrado en la base de datos del **SERVICIO**, que la persona está solicitando licencia de conducir en **LA MUNICIPALIDAD**, evitando con ello la multiplicidad de solicitudes en distintos municipios.

3. Certificado de Multas del Tránsito no Pagadas

- Veinte (20) puestos de trabajo estarán ubicados en el Juzgado de Policía Local, desde el cual sólo se podrá acceder a:

1. Emisión de Documentos Electrónicos

Cada Juzgado de Policía Local de la comuna a que pertenece **LA MUNICIPALIDAD** podrá emitir los certificados, documentos e informes electrónicos no valorados, que a continuación se señalan:

1. Certificado de Anotaciones Vigentes del Registro de Vehículos Motorizados.
2. Certificados de Antecedentes de Conductor, el cual se utilizará sólo para la obtención de duplicados de Licencias de Conducir extraviadas, o destruidas total o parcialmente, de acuerdo con lo establecido en el artículo 29, de la Ley N°18.290, de Tránsito.
3. Extracto de Filiación y Antecedentes, el cual podrá ser solicitado sólo por el Juzgado de Policía Local, y con la finalidad única y exclusiva de obtener la información a que se refiere el artículo 2°, del Decreto Ley N°645, de 1925, sobre Registro General de Condenas.
4. Extracto de Inscripción en el Registro de Vehículos Motorizados, el cual sólo podrá ser solicitado por el funcionario del Juzgado de Policía Local debidamente autorizado por el Juez, y por los Inspectores Municipales, de acuerdo con lo dispuesto en el artículo 3°, de la Ley N°18.287, que Establece Procedimiento ante los Juzgados de Policía Local y sólo para los efectos que dicha norma señala.
5. Certificado de Multas del Tránsito no Pagadas, el cual tendrá incluida la siguiente leyenda "Para uso exclusivo de Juzgado de Policía Local".
6. Informe de Domicilio de uso exclusivo para Instituciones Públicas y Tribunales, cuya información en él contenida, será utilizada en forma restringida por el Juzgado de Policía Local, a fin de dar cumplimiento exclusivamente a las funciones asignadas por la Ley N°18.290 y sus posteriores modificaciones.

2. Consultas a la Base de Datos.

Los Juzgados de Policía Local de la comuna a que pertenece **LA MUNICIPALIDAD** podrán acceder a la consulta de la base de datos del **SERVICIO**, que a continuación se señala:

1. Inscripciones de Nacimiento: Se realizarán consultas por nombre y RUN, se desplegará toda la información de nacimiento: datos del inscrito (RUN, y nombre completo), fecha de nacimiento, datos de la inscripción (circunscripción, número de inscripción, tipo de registro, año de la inscripción), datos de los padres (RUN y nombre completo en caso de existir), RUN de hijos asociados (en caso de existir).
2. Inscripciones de Matrimonio: Se realizarán consultas por nombre y RUN, se desplegará toda la información del matrimonio: datos de los cónyuges (RUN y nombre completo), datos de la inscripción (circunscripción, número de inscripción, tipo de registro, año de la inscripción), fecha y hora de celebración de matrimonio, régimen patrimonial del matrimonio y subinscripciones realizadas.
3. Inscripciones de Defunción: Se realizarán consultas por nombre y RUN, se desplegará toda la información de la defunción: datos del inscrito (RUN y nombre completo), fecha de defunción, datos de la inscripción (circunscripción, número de inscripción, tipo de registro, año de la inscripción).
4. Inscripciones en el Registro de Vehículos Motorizados: Se realizarán consultas a través del RUN del propietario o a través de la Placa Patente Única de los vehículos, desplegará información de datos de vehículo: marca, modelo, año fabricación, color, número chasis, número motor, datos del propietario: RUN, nombre, domicilio, datos de anotaciones, limitaciones al dominio y dueños anteriores.

Por otra parte, **EL SERVICIO**, una vez desarrolladas, disponibilizará las funcionalidades vinculadas al Ingreso en Línea de Resoluciones Judiciales en el Registro Nacional de Conductores (RNC) y al Preingreso de Eliminaciones Judiciales en el Registro de Multas de Tránsito No Pagadas (RMTNP).

- Cien (100) de trabajo estará ubicado en la Inspección Municipal, desde el cual sólo se podrá acceder a:

1. Extracto de inscripción en el Registro de Vehículos Motorizados.
2. Certificado de Multas de Tránsito no pagadas.

Tal como se señaló anteriormente, **LA MUNICIPALIDAD** también podrá emitir a través del Sistema de Gestión de Licencias de Conducir (SGL) los siguientes certificados del **SERVICIO**:

3. Certificado de Antecedentes Conductor de uso exclusivo para obtención o renovación de Licencias de conductor.
4. Certificado de Antecedentes Conductor de uso exclusivo Juzgados de Policía Local y Municipalidades.

QUINTA: Cuentas de acceso.

La persona encargada de coordinar, designada por **LA MUNICIPALIDAD,** a través del Formulario de Solicitud de Cuentas Computacionales para el acceso al aplicativo Monito Web definido por **EL SERVICIO;** solicitará a la Plataforma Usuarios del **SERVICIO**, creación de las cuentas habilitadas de los usuarios, para efectos de conectarse a la red corporativa del **SERVICIO,** a través del correo electrónico cuentas@registrocivil.gob.cl.

Estas cuentas tendrán los privilegios requeridos para la emisión de los documentos electrónicos y consultas a la base de datos definidos en la cláusula CUARTO: "Acceso y Puestos de Trabajo".

Dichas cuentas computacionales, tendrán el carácter de secretas, personales, indelegables e intransferibles, y su mal uso acarreará la responsabilidad administrativa que corresponde a toda persona funcionaria municipal, la que deberá perseguirse y hacerse efectiva por **LA MUNICIPALIDAD**, de conformidad con lo dispuesto en la Ley N°18.883, que Aprueba el Estatuto Administrativo para Funcionarios Municipales, sin perjuicio de las eventuales responsabilidades civiles y penales a que hubiere lugar.

En caso que **LA MUNICIPALIDAD** solicitare un aumento de los puestos de trabajo, deberá suscribirse un Anexo entre las partes, el que deberá ajustarse a lo dispuesto en la Cláusula DÉCIMO NOVENO: "Anexos" del presente Convenio.

Asimismo, **LA MUNICIPALIDAD** estará obligada a comunicar por escrito al **SERVICIO**, el cambio de personas funcionarias designadas para los efectos antes señalados, a través del Formulario individualizado precedentemente.

El incumplimiento de comunicar a la persona encargada de coordinar del **SERVICIO** la designación o el cambio de la persona encargada de coordinar designada por **LA MUNICIPALIDAD**, facultará al **SERVICIO** para poner término en forma inmediata al presente Convenio de Adhesión.

Por otra parte, el acceso al Sistema de Gestión de Licencias de Conducir (SGL) serán aquellos definidos e informados por la Subsecretaría de Transportes a **LA MUNICIPALIDAD**, cuyas consultas deberán realizarse directamente a la casilla de correo electrónico mejoresconductores@mtt.gob.cl.

SEXTA: Limitaciones en el uso de la Información.

LA MUNICIPALIDAD 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 MUNICIPALIDAD** 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.

LA MUNICIPALIDAD 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, la persona encargada de coordinar de **LA MUNICIPALIDAD** deberá enviar copia de dicha instrucción y/o de los respectivos contratos a la persona que esté encargada de coordinar del **SERVICIO.**

En consecuencia y especialmente, **LA MUNICIPALIDAD** 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 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 MUNICIPALIDAD** deberá velar por el cumplimiento 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 MUNICIPALIDAD** dará derecho al **SERVICIO** para poner término anticipado al presente convenio.

SÉPTIMA: Precio.

Los valores que **LA MUNICIPALIDAD** deberá pagar por la prestación de servicios que se establecen en el presente convenio, corresponden sólo al concepto de emisión de certificados de aquellos que tengan el carácter de valorados, los que serán fijados por decreto del Ministerio de Justicia y Derechos Humanos.

Conforme a lo anterior, será obligación de **LA MUNICIPALIDAD**, de igual forma exigible el pago por los certificados valorados emitidos tanto a través del aplicativo Monito Web como del Sistema de Gestión de Licencias de Conducir (SGL), lo que deberá realizarse en forma oportuna y total conforme a las obligaciones de pago que se establecen en el presente convenio.

OCTAVA: Forma y oportunidad de pago.

Los certificados emitidos por la Dirección de Tránsito y Transporte Público para otorgar licencias de conducir que tengan el carácter de valorados deberán ser pagados por **LA MUNICIPALIDAD** en un plazo de diez (10) días hábiles contados desde la recepción del oficio emanado por la Unidad de Finanzas de la Dirección Regional correspondiente, el cual contemplará en adjunto el detalle de los certificados emitidos por **LA MUNICIPALIDAD** del mes respectivo.

LA MUNICIPALIDAD se obliga a pagar el total de los certificados emitidos mensualmente independientemente del medio utilizado para su emisión, mediante transferencia electrónica o depósito bancario a nombre del Servicio de Registro Civil e Identificación, en la cuenta corriente "Ingresos" de la Dirección Regional respectiva, debiendo indicar en la glosa de la transferencia o deposito, el número y fecha del Oficio enviado por la Unidad de Finanzas de la Dirección Regional, mediante el cual se requirió el pago de los Certificados, y que se están pagando a través de la respectiva transferencia. El comprobante de dicha transferencia o deposito deberá ser enviada al correo electrónico de la Dirección Regional correspondiente, el mismo día de realizada la transacción. Para efectos de lo anterior, tanto el número de la cuenta corriente como el correo electrónico de la Dirección Regional, serán informados por la Unidad de Finanzas respectiva.

NOVENA: Operatividad.

Las partes acuerdan que será responsabilidad de **LA MUNICIPALIDAD**, y a su costo, la implementación, mantención y reparación del mecanismo que permite hacer operable el aplicativo Monito *Web* que da cuenta el presente Convenio de Adhesión.

Respecto del Sistema de Gestión de Licencias de Conducir (SGL) serán aquellas condiciones definidas e informadas por la Subsecretaría de Transportes a **LA MUNICIPALIDAD**.

DÉCIMA: Asistencia

El Subdepartamento de Atención de Instituciones del **SERVICIO** proveerá y/o gestionará la correspondiente asistencia que requiera **LA MUNICIPALIDAD,** para efectos de la implementación del acceso al aplicativo monito web, a través del correo electrónico convenios@registrocivil.gob.cl con copia a soporteconvenios@registrocivil.gob.cl

La persona encargada de coordinar del **SERVICIO** informará anualmente a la persona encargada de coordinar de **LA MUNICIPALIDAD,** los teléfonos de contacto para efectos de fortalecer la comunicación antes señalada.

Por otra parte, para la asistencia del Sistema de Gestión de Licencias de Conducir (SGL), **LA MUNICIPALIDAD** deberá remitir las consultas correo mejoresconductores@mtt.cl.

UNDÉCIMA: Uso publicitario.

Todo uso publicitario que **LA MUNICIPALIDAD** quisiera hacer respecto de la entrega de datos objeto del presente Convenio de Adhesión deberá contar con la autorización escrita del **SERVICIO**, evento en el cual **LA MUNICIPALIDAD** deberá indicar los fines, el medio de difusión y el destinatario. Su incumplimiento será causal de término del convenio contemplado en la Cláusula DÉCIMO SEXTO "Término Anticipado".

DUODÉCIMA: Propiedad y exclusividad del Aplicativo Monito *Web* u otro.

Para los efectos del presente Convenio de Adhesión, se considerará propiedad del 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 propiedad o proporcionadas por éste, relacionado con la materia y el aplicativo Monito Web u otro mecanismo que defina en el futuro, todo lo cual, además, constituye información confidencial.

DÉCIMA TERCERA: Continuidad del servicio.

Toda mantención, readecuación o interrupción de la operación del aplicativo Monito Web u otro que defina en el futuro **EL SERVICIO**, programada o no, deberá ser comunicada oportunamente, por parte de la persona encargada de coordinar del **SERVICIO** mediante correo electrónico a la persona encargada de coordinar definida por **LA MUNICIPALIDAD**.

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

DÉCIMA CUARTA: Daños y perjuicios vinculados.

EL SERVICIO queda liberado de toda responsabilidad por los daños directos e indirectos, perjuicios previstos o imprevistos, de cualquier naturaleza que pueda experimentar **LA MUNICIPALIDAD**, como consecuencia directa de la información proporcionada.

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

DÉCIMA QUINTA: Duración y vigencia.

El presente Convenio de Adhesión 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/ a la Alcalde de **LA MUNICIPALIDAD** o al Director Nacional del **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.

DÉCIMA SEXTA: Término Anticipado.

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

1. Que, **LA MUNICIPALIDAD**, o la persona funcionaria de su dependencia, que acceda a la información materia del presente Convenio de Adhesión, no mantengan la debida reserva de la información considerada confidencial.
2. Que, **LA MUNICIPALIDAD** no comunique por escrito al **SERVICIO**, el cambio de personas funcionarias designadas para los efectos de conectarse al aplicativo Monito *Web* u otro que en el futuro determine **EL SERVICIO** establecido en la cláusula QUINTO.
3. Que, por cesar en sus funciones **LA MUNICIPALIDAD** que suscribe el presente Convenio de Adhesión, éste o la persona encargada de coordinar designada en la cláusula DÉCIMO SÉPTIMO "Personas encargadas de coordinar", no dé aviso de este hecho al **SERVICIO**, con al menos diez (10) hábiles de anticipación.
4. Que, el servicio permanezca interrumpido o sin uso por parte de **LA MUNICIPALIDAD**, por más de tres (3) meses consecutivos.
5. Que, en general, no se cumpla con alguna de las condiciones u obligaciones estipuladas en el presente Convenio.
6. Por acuerdo de las partes.
7. Por exigirlo el interés público o la seguridad nacional.
8. Que, se verifique la existencia de leyes, decretos, reglamentos, o sentencias judiciales que regulen toda o alguna 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 los servicios que por este Convenio se regula.

DÉCIMA SÉPTIMA: Personas encargadas de coordinar.

Con el objeto de velar por el fiel cumplimiento del presente Convenio, y en lo que respecta exclusivamente a la utilización y operatividad del aplicativo Monito *Web*, cada una de las partes designará una persona encargada de coordinar:

- Por **EL SERVICIO**:
  El Director Regional (S) Metropolitano de **EL SERVICIO**, don Luis Díaz Mansilla, correo electrónico [redacted], fono (2261) 14302 o quien le subrogue en el cargo.

- Por **LA MUNICIPALIDAD**:
  La Jefa de Departamento de Licencias de Conducir de **LA MUNICIPALIDAD**, doña Ingrid Carrasco Pérez, correo electrónico [redacted] fono (22) 6543391 o quien le subrogue en el cargo.

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

DÉCIMA OCTAVA: Copias.

Se deja constancia que el presente Convenio de Adhesión se firma en dos (2) ejemplares de igual tenor y fecha, quedando uno (1) en poder de cada parte.

DÉCIMA NOVENA: Anexos.

Las partes acuerdan que en el evento de ser necesario suscribir algún Anexo, éste se entenderá formar parte integrante del presente Convenio de Adhesión, lo que deberá ser aprobado mediante Resolución del Director Nacional del S**ERVICIO** y del/ de la Alcalde de la comuna de **LA MUNICIPALIDAD**.

VIGÉSIMA: Solución de conflictos.

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

VIGÉSIMA PRIMERA: Personerías.

La personería de don Omar Morales Márquez para actuar a nombre y en representación del **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.

La personería de don Jaime Bellolio Avaria, para actuar a nombre y en representación de **LA MUNICIPALIDAD**, consta de Decreto N°3247 de fecha 06 de diciembre de 2024 de la Municipalidad de Providencia.

OMAR MORALES MÁRQUEZ **DIRECTOR NACIONAL** **SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN**	**JAIME BELLOLIO AVARIA** **ALCALDE** **MUNICIPALIDAD DE PROVIDENCIA**

VHD /CCC / AMC/ DSP

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

ELABORADO POR	REVISADO POR	REVISADO POR	APROBADO POR
Andrea Muñoz Contreras Jefa Subdepartamento de Atención de Instituciones	Soledad Ávila Soto Subdirectora Jurídica (S)	Cirus Quiernas Sánchez Jefe Departamento de Gestión Institucional, Transparencia, Ciudadanía	Omar Morales Márquez Director Nacional

V°B Constanza González Gacitúa

V°B° Gabriela Basoalto López

V°B° María Cecilia Ríos Suazo – Encargada de Seguridad de la Información

V°B° Álvaro Caré Caro – Encargado de Ciberseguridad

REVISIONES DEL PROCEDIMIENTO			
N° Versión	**Fecha**	**Motivo de la revisión**	**Páginas elaboradas o modificadas**
0 (cero)	31/10/2012	Elaboración inicial de la Política de Convenios Asociados a la Prestación de Servicios de Verificación y/o Transferencia de información con Instituciones de acuerdo a los lineamientos del Sistema de Seguridad de la Información (SSI) y los requisitos de las normas NCh-ISO 27001:2013.	Todas.
N°1 (uno)	24/08/2015	Se ajusta el documento en los Principios de la Política.	Todas.
N°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.
N°3 (tres)	26/04/2019	Se revisa número de versión de política. Se valida el contenido de la política y se actualizan los contenidos.	Todas.
N°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.
N°0 (cero)	19/04/2021	Se redefine la política, la cual pasa a denominarse: Política de Protección de Datos Personales para la Transferencia o verificación de datos a terceros. Este documento reemplaza a la Política de Convenios Asociados a la Prestación de Servicios de Verificación y/o Transferencia de Información con Instituciones. 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.
N°01 (uno)	09/01/2024	Actualización de contenidos, en base a cambio de dependencia establecida en la Resolución Exenta N°283, de 28 de junio 2023. Ajuste de formato en base al PR-47-SGSPI Procedimiento Elaboración de Documentos del SIGESPI, versión 0, aprobada por Resolución Exenta N°353 del 23 de agosto de 2023.	Todas.

I. DECLARACIÓN INSTITUCIONAL

El Servicio de Registro Civil e Identificación (SRCeI), dentro de su Sistema de Gestión de Seguridad y Privacidad de la Información define como prioritario el proteger los datos personales contenidos en sus activos de información, a fin de asegurar la continuidad de los procesos de la Institución, y así poder eliminar o minimizar el daño que se les pudiera producir a estos activos, conforme a su Política de Seguridad y Privacidad de la Información y en la normativa vigente en el país.

II. OBJETIVO GENERAL

La presente política tiene por objetivo formular las directrices generales de protección de los datos en los procesos de verificación o transferencia de información a terceros, minimizando el impacto de los riesgos externos estableciendo 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 Política de Transformación Digital del Estado.

III. OBJETIVOS ESPECÍFICOS

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:

i. Resguardar la confidencialidad, integridad y disponibilidad de la información tratada, procesada y almacenada por el SRCeI.

ii. Proteger la privacidad de la Información de Identificación Personal (PII) contenida en los activos de información del SRCeI.

iii. Fortalecer la implementación de una cultura de seguridad de la información en el SRCeI.

iv. Garantizar la continuidad operacional, frente a incidentes de seguridad y privacidad de la información, gestionándolas de forma oportuna e implementando las acciones correctivas que correspondan.

v. 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.

vi. Fortalecer el rol del SRCeI como organismo público de la Administración del Estado en la satisfacción de las necesidades colectivas y el bien común.

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

viii. Generar alianzas estratégicas con otros organismos e instituciones, creando sinergias que permitan mejorar la entrega de los servicios a los/las usuarios/as.

IV. ALCANCE

La presente política orienta su acción a regular la verificación o transferencia de información desde el SRCeI a las distintas Instituciones Públicas y/o Privadas, en cuanto a la celebración de convenios, estableciendo la protección de datos personales.

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 de suplente o reemplazo; al personal contratado a honorarios y a los terceros (incluyendo contratistas) que interactúen de manera habitual u ocasional con la Institución, debiendo constar en sus respectivos contratos las cláusulas de protección de datos, confidencialidad y limitaciones en el uso de la información.

V. REFERENCIAS

- Artículo 19 N°4, de la Constitución Política de la República de Chile.
- Ley N°19.628, sobre Protección de la Vida Privada.
- Ley N°19.477, Orgánica del Servicio de Registro Civil e Identificación, del Ministerio de Justicia.
- Ley N°19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma.
- Ley N°20.285, sobre Acceso a la Información Pública.
- Ley N°21.180, sobre Transformación Digital del Estado.
- Ley N°21.459, que 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 Supremo N°83, de 2005, de la Secretaría General de la Presidencia, que aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.

- Decreto Supremo N°273 del 13 de septiembre de 2022, en cuanto a notificar sobre los incidentes de ciberseguridad que afecten al SERVICIO al Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior y Seguridad Pública, CSIRT.
- Decreto Supremo N°12 que Establece Norma Técnica de Interoperabilidad, del 17 de agosto de 2023, del Ministerio Secretaría General de la Presidencia.
- Decreto Supremo N°164, del 4 de diciembre de 2023, que Aprueba Política Nacional de Ciberseguridad 2023-2028, del Ministerio del Interior y Seguridad Pública y Subsecretaría del Interior.
- Decreto Supremo N°1299 que Establece Nuevas Normas que Regulan la Red de Conectividad del Estado que Administra el Ministerio del Interior y Fija los Procedimientos, Requisitos y Estándares tecnológicos para la Incorporación a dicha Red de Instituciones Públicas, de 29 de abril de 2005, del Ministerio del Interior, Subsecretaría del Interior.
- Resolución Exenta N°304, de fecha 30 de noviembre de 2020, que aprueba el Texto Actualizado y Refundido de las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado y sustituye texto que indica.
- Resolución Exenta N°323, de fecha 04 de julio de 2022, Composición del Comité Directivo de Seguridad de la Información.
- Instrucción N°10, Sobre el Procedimiento Administrativo de Acceso a la Información, Consejo para la Transparencia, de fecha 28 de octubre de 2011.
- Norma NCh-ISO 27001:2013 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos. Anexo A, control A.13.2.2 Acuerdos sobre la transferencia de información.
- Norma NCh-ISO 27002:2013 Tecnologías de la información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información. Control. 13.2.1 Políticas y procedimientos sobre la transferencia de información, 13.2.2 Acuerdos sobre la transferencia de información.
- Norma NCh-ISO 27701:2020 Técnicas de Seguridad – Extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad – Requisitos y directrices. Control A.7.5 Intercambio, transferencia y eliminación de PII, B.8.5 Intercambio, transferencia y eliminación de PII.

VI. DEFINICIONES

Término	Definición
Activo de Información del SRCEI	Son todos los registros que la ley ha encomendado al SRCEI su administración y custodia, los que contienen información de valor para la institución en distintos soportes físicos y digitales. Se distinguen tres niveles de información: • 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.

Término	Definición
	• Los funcionarios que tienen el conocimiento de los procesos institucionales.
Comité Directivo de Seguridad y Privacidad	Es el equipo conformado por jefaturas de las áreas de la institución, responsable de la toma de decisiones en temas de la seguridad y privacidad de la información, quienes han sido designados por la Resolución N°323, de fecha 04 de julio de 2022
Confidencialidad funcionarios SRCel	Personal del SRCel deberá guardar la debida reserva de los antecedentes o documentos de los cuales tome conocimiento en el cumplimiento de sus labores, sin perjuicio de las informaciones y certificaciones que deba proporcionar el Servicio en conformidad a la ley
Almacenamiento de Datos	Es la conservación o custodia de datos en un registro o bancos de datos
Bloqueo de datos	Es la suspensión temporal de cualquier operación de tratamiento de los datos almacenados
Comunicación o transmisión de datos	Dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.
Dato caduco	Es el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o expiración del plazo señalado para su vigencia, si no hubiere norma expresa, por el cambio de los hechos o circunstancias que consigna.
Dato estadístico	Es el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable (Estadísticas Vitales).
Dato personal	Son los datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables (Datos Cédula de Identidad: Nombre, RUN, Domicilio)
Dato sensible	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 (ejemplo: Registro Nacional de la Discapacidad).
Fuentes accesibles al público	Son los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

Término	Definición
Fuentes no accesibles al Público	La naturaleza de los registros en poder del Servicio de Registro Civil e Identificación, si bien son registros públicos, no constituyen una fuente de acceso público, esto es, aquella a la cual toda persona puede acceder sin restricciones de ningún tipo. En efecto, la circunstancia de que, para acceder al contenido de determinada información en poder del organismo requerido, se deba proporcionar datos como; el nombre o la cédula identidad, supone, necesariamente, excluir dichos registros, de la calificación de fuentes de libre acceso público (Consejo en las decisiones de amparos Roles C1519-15 y C2138-18).
Registro o banco de datos	Es el conjunto, organizado de datos de carácter personal, sea automatizado o no y cualquier forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos
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.
Jefes de Área	Subdirectores(as), Jefes(as) de Departamento, Jefes(as) de Unidades dependientes de la dirección nacional, Directores(as) Regionales.
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 de acceso a la información	Actos por el que las instituciones públicas o privadas que interactúan con el SRCel solicitan información. (Fuente Consejo para la Transparencia).
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.

Término	Definición
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 / Trabajador	Funcionario es toda persona que tenga un vínculo contractual de trabajo con SRCel de Planta, Contrata, Suplente o Reemplazo. Trabajador/a contratado a Honorario o Código del Trabajo.

VII. ROLES Y RESPONSABILIDADES

Rol	Responsabilidad
Director/a Nacional	▪ Definir la procedencia de incorporar multas y garantías de fiel cumplimiento de los convenios para cautelar los recursos públicos. ▪ Proveer los medios para la implementación de esta Política. ▪ Aprobar las versiones actualizadas de esta Política.
Subdirección Jurídica	▪ Recomendaciones a la presente Política. ▪ Revisar la legalidad de las cláusulas de los convenios de transferencia o verificación de datos. ▪ Determinar la procedencia de emitir pronunciamientos jurídicos previos a la celebración de convenios con instituciones públicas o privadas. ▪ Determinar el contenido jurídico de los convenios y, en particular, de los convenios tipo.
Subdirección de Administración y Finanzas	▪ Informar al Subdepartamento de Atención a Instituciones sobre el incumplimiento del pago de los servicios por parte de instituciones privadas. ▪ Pronunciarse sobre el monto de las multas que se pactarán en los convenios según los distintos tipos de incumplimiento, fijando los topes máximos de aplicación de las mismas que darán lugar al término anticipado del convenio y al cobro de la garantía de fiel cumplimiento, en su caso. ▪ Custodia de instrumentos de Garantía de Fiel Cumplimiento de los convenios.

Rol	Responsabilidad
Encargado/a de Seguridad y Privacidad de la Información (ESI)	▪ Participar en la revisión de la presente política. ▪ Difundir y sensibilizar respecto de la presente política.
Encargado/a de Ciberseguridad	▪ Participar en la revisión difusión y sensibilización de las políticas y procedimientos de Ciberseguridad relacionados con la transferencia o verificación de datos personales a terceros. ▪ Realizar recomendaciones para la mejora continua del proceso de transferencia o verificación de datos a terceros.
Subdirector/a de Estudios y Desarrollo	▪ 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.
Jefe/a del Departamento de Gestión Institucional, Transparencia, Ciudadanía y Patrimonio	▪ Revisar la presente política. ▪ Aprobar los procedimientos necesarios para la implementación de esta política. ▪ Verificar que los convenios de transferencia o verificación de datos a terceros contengan cláusulas relativas a la seguridad y privacidad de la información
Jefe(a) del Subdepartamento 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. ▪ Informar eventos o incidentes de seguridad de la información que digan relación con los convenios de transferencia o verificación de datos a terceros. ▪ Gestionar la revisión de los plazos de vigencia de los convenios, controlando que su renovación o término, se formalice oportunamente. ▪ Gestionar la aplicación de multas por incumplimiento de las instituciones privadas, de acuerdo a la información proporcionada por la Subdirección de Administración y Finanzas. ▪ Incorporar cláusulas de término anticipado en todos los convenios. ▪ Función de Coordinadora de los Convenios. ▪ Informar a la Subdirección Jurídica las deudas que registre la institución privada previo a requerir el término de los convenios o su renovación. ▪ Revisión y control de la vigencia de los instrumentos de garantía de fiel cumplimiento de los convenios.

Rol	Responsabilidad
Jefes de Registros (Dueños del Proceso)	▪ Informar, previo a la emisión del respectivo pronunciamiento jurídico por parte de la Subdirección Jurídica, sobre la procedencia y formato de la entrega de la información solicitada, en caso de estimarse procedente la entrega. ▪ Dejar trazabilidad escrita de 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, entre otras.

VIII. LINEAMIENTOS

- 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.

- Será responsabilidad de las jefaturas que administran los registros, dejar trazabilidad escrita de 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, entre otras.

- 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.

- Todo acuerdo relativo a la transferencia o verificación de datos personales a terceros debe considerar cláusulas que garanticen el uso de la información únicamente para el cumplimiento de los propósitos establecidos en los convenios suscritos, en conformidad a las competencias legales en el caso de Instituciones Públicas o que digan directa relación con su giro en el caso de las Instituciones Privadas.

- 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 SRCel, 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, copia, total o parcial; modificación, ruteo incorrecto, revelación, publicación, difusión, venta, cesión, reproducción, interferencia, intercepción, alteración, daño, inutilización y/o destrucción.

  - Proteger la información electrónica sensible comunicada en forma de elemento adjunto.

- Se deberá incorporar equidad de género, protección a la infancia, protección al adulto mayor y protección del medio ambiente, así como también, lo establecido en la Política Nacional de Ciberseguridad del 4 de diciembre de 2023; en el contenido de los convenios que se suscriban, asimismo se incentivará a las instituciones suscriptoras 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 los servicios de transferencia o verificación de datos que el SRCel les pueda proporcionar.

- Se deberá mantener una cartera actualizada de los servicios de verificación o transferencia de datos a terceros y un Catálogo de Servicios de Interoperabilidad, según se establece en el Decreto N°12 de agosto de 2023, disponible para Instituciones Públicas y/o Privadas.

- Con todo, se prohíbe el traspaso de 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.

IX. DIFUSIÓN

Conforme lo establecido en PR-47-SGSPI Procedimiento elaboración documentos del SIGESPI, se mantendrá a disposición de los funcionarios/as, proveedores, contratistas y terceros, la versión actualizada de la POL-15-SGSPI Política de Protección de Datos Personales para la Transferencia o verificación de datos a terceros en la Intranet institucional (https://intranet.beta.srcei.cl/)

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.

X. VIGENCIA Y REVISIÓN

La presente política será evaluada y revisada al menos una vez al año por el Departamento de Gestión Institucional, Transparencia, Ciudadanía y Patrimonio, 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.

XI. SANCIONES POR INCUMPLIMIENTO

Frente al incumplimiento o violación de la presente política; se aplicará lo establecido en PR-38-SGSPI Procedimiento Sanciones por Incumplimiento de las Políticas y Normativas asociadas a la Seguridad de la Información.

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 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ELABORADO POR	REVISADO POR	APROBADO POR
M. Cecilia Ríos Encargada de Seguridad de la Información	Mauricio Cornejo Catalán Jefe Unidad de Gestión Estratégica	Omar Morales Márquez Director Nacional

V°B° Jorge Núñez Silva, Subdirector de Operaciones

V°B° Rodrigo Llambias Lascar, Subdirector Jurídico (S)

V°B° Daniel Teplizky Barahona, Subdirector de Estudios y Desarrollo (S)

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 noma 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	Todas

N° de Versión	Fecha	Motivo de la revisión	Páginas elaboradas o modificadas
		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.	
N°07 (siete)	16/03/2023	Revisión anual de la política según norma NCh-ISO/IEC 27001:2013. Incorporación de los siguientes cuerpos legales: - Ley N°21.459 que 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° 273 del 13 de septiembre de 2022, en cuanto a notificar sobre los incidentes de ciberseguridad que afecten al SERVICIO al Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior y Seguridad Pública, CSIRT. - Instructivo Presidencial N°001, de 19 de febrero de 2018, sobre la evaluación y adopción preferente de servicios en la nube por parte de los órganos de la	

N° de Versión	Fecha	Motivo de la revisión	Páginas elaboradas o modificadas
		Administración Central del Estado. Incorpora oportunidad de mejora levantada en Informe de auditoría Fase1_v1 realizada por consultora ITQ en diciembre de 2022: "(...) se recomienda establecer o incorporar un objetivo específico de seguridad de la información a nivel de gestión de riesgo y definir si la protección de activos será sobre todos los del SERVICIO o si solo será sobre los críticos. Aunado a ello, se recomienda revisar y redefinir el objetivo 9 de la política en conjunto con el objetivo 7".	

1. OBJETIVO

Establecer los lineamientos para gestionar la seguridad y privacidad de la información en el Servicio de Registro Civil e Identificación, en adelante el SERVICIO

2. OBJETIVOS ESPECÍFICOS

i. Propender a la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información.
ii. Resguardar la confidencialidad, integridad y disponibilidad de la información tratada, procesada y almacenada por el SERVICIO.
iii. Proteger la privacidad de la Información de Identificación Personal (PII) contenida en los activos de información del SERVICIO.
iv. Establecer la gobernanza de seguridad de la información, segregando roles y responsabilidades para gestionar los accesos a los activos de la información de para su adecuada protección de acuerdo con los niveles de clasificación.
v. Establecer una estructura de seguridad y privacidad de la información por medio de un marco de políticas, estándares y procedimientos en materia de seguridad de la información.
vi. Fortalecer la implementación de una cultura de seguridad de la información en el SERVICIO.
vii. Apoyar las garantías de la continuidad del negocio frente a incidentes de seguridad y privacidad de la información gestionándolas de forma oportuna e implementando las acciones correctivas que correspondan.

3. 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; y respecto del personal contratado a honorarios; **y terceros** (incluyendo contratistas y suscriptores de convenios) que interactúen de

manera habitual u ocasional con la institución, los cuales deberán contener en sus contratos.

En cuanto a los procesos que forman parte del SGSPI, se identificarán en el documento

4. REFERENCIAS

- Constitución Política de la República de Chile artículo 19 N°4.
- D.F.L. N°1/ 19.653, que fija Texto Refundido, Coordinado y Sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
- Ley N°19.880, Establece Bases de los Procedimientos Administrativos que Rigen Los actos de los Órganos de la Administración del Estado.
- Ley N°19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y sus modificaciones.
- Ley N°19.477. Orgánica del Servicio de Registro Civil e Identificación.
- Ley 21.180, sobre Transformación Digital del Estado.
- Ley N° 21.459, que establece normas sobre delitos informáticos, que deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.
- Ley N° 19.628, sobre Protección de la Vida Privada.
- LEY N°20.393 establece la responsabilidad penal de las personas jurídicas en los delitos que indica.
- Ley n°19.799. sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

- DFL N°4, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N°19.039, de Propiedad Industrial.

- Decreto Supremo N° 250, de 2004, del Ministerio de Hacienda, que aprueba el Reglamento de la Ley N° 19.886 y sus modificaciones;

- decreto supremo n°83, de 2005, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos, del Ministerio Secretaría General de la Presidencia,

- Decreto N° 273, que establece obligación de reportar incidentes de ciberseguridad, del Ministerio del Interior y Seguridad Pública, Subsecretaría del Interior.

- Instructivo Presidencial N°001 de 2018, que Imparte instrucciones sobre Transformación digital en los órganos de la Administración del Estado, de Presidencia.

- Instructivo del Gabinete Presidencial N°008 del 23 de octubre de 2018 que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado.

- 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 los procesos que pudiesen poner en riesgo los activos de la información y a su vez la protección de datos personales y sensibles, y serán identificados en el documento **REG-07-SGSPI SOA_Declaracion_Aplicabilidad**.

5. 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

Término	Definición
	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.
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, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. En el caso del SRCel, 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

Término	Definición
	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.
Política	Directriz u orientación general expresada formalmente por la Alta Dirección del Servicio.
Privacidad	Desde el punto de vista normativo (NCh-ISO 27001:2013, NCh-ISO 27701:2020) se refiere a los requerimientos para salvaguardar la privacidad en cualquier sistema en el que se procese información de identificación personal y servir como complemento en el caso que existan consideraciones legales relacionadas. La privacidad de los datos significa la capacidad de una persona para determinar por sí misma cuándo, cómo y hasta qué punto se comparte o se comunica a otros su información personal. Esta información personal puede ser el nombre, la ubicación, la información de contacto o el comportamiento en línea o en el mundo real.
Procedimiento	Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad y Privacidad de la Información.
Responsable de la Información y Privacidad de los datos	Es el(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.

Término	Definición
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. En el caso la gestión de la Seguridad de la Información forma parte del Sistema de Seguridad y Privacidad de la Información del SERVICIO.
Sistema de Gestión en Privacidad de la Información (SGPI)	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 SRCeI, 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.

Término	Definición
Funcionario(a) / Trabajador(a)	Toda persona que tenga un vínculo contractual de trabajo con SRCeI, independiente de la calidad jurídica: Planta, Contrata, Honorario, Código del Trabajo.
Tratamiento	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
Vulnerabilidad	Debilidad de un activo o grupo de activos que puede ser materializada por una o más amenazas.

6. ROLES Y RESPONSABILIDADES

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

Rol	Responsabilidad
Director/a Nacional	(a) Proveer los medios para la implementación de esta Política de Seguridad y Privacidad de la Información. (b) Aprobar las versiones actualizadas de esta Política.
Comité Directivo de Seguridad de la Información (CDS),	(a) Revisar, aprobar y difundir la presente política. (b) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes de seguridad que se desprendan de esta política.
Comité Operativo de Seguridad de la Información (COS),	(a) Proponer y supervisar la implementación de procedimientos y estándares que se desprendan de esta política.
Encargado/a de Seguridad de la Información (ESI)	(a) Difundir y sensibilizar respecto de la Política de Seguridad y Privacidad de la Información a los funcionarios/as de la institución.
Jefatura Unidad Control de Riesgos y Seguridad TI	(a) Generar la definición y materialización de los planes de corto, mediano y largo plazo relativos a la Seguridad de la Información y Seguridad y Privacidad de la Información.
Encargado/a de Ciberseguridad	(a) Gestionar los riesgos asociados a Ciberseguridad relacionados con esta política.

Rol	Responsabilidad
Encargados/as de Seguridad de la Información Regionales	(a) Asesorar al Director/a Regional, respecto de la presente política y procedimientos o instrucciones de trabajo que se desprendan de ella, así como a todos los funcionarios y funcionarias de la región.
Responsable del tratamiento de los datos personales	(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 sea veraz, completa, exacta, actualizada, comprobable y comprensible. (d) Actualizar la información, 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.

Un mayor detalle de las responsabilidades y funciones de los roles que componen la estructura del SGSPI se encontrarán descritas en los 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 terceros contratados que prestan servicios, que tengan acceso a los activos de información del SERVICIO, 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 SGSPI.

7. LINEAMIENTOS

7.1. DECLARACIÓN INSTITUCIONAL.

El Servicio de Registro Civil e Identificación, en adelante el SERVICIO, 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, ha implementado un Sistema de Gestión de Seguridad y Privacidad de la Información (en adelante, SGSPI) 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 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).

7.2. 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 Nº 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.

7.2.1. 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.

De esta manera, 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.

7.2.2. Titular de los Datos Personales.

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

a) Información de los bancos de datos de responsabilidad del SERVICIO, 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.

7.2.3. Deberes del SERVICIO como responsable del tratamiento de Datos Personales.

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 SERVICIO- 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 SERVICIO 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 SERVICIO o por terceros contratados por él 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.

8. DIFUSIÓN

La presente versión se encontrará disponible en la Intranet institucional (https://intranet.beta.srcei.cl) y en el sitio web institucional (https://www.registrocivil.cl/principal/quienes-somos/politica-de-seguridad).

Sin perjuicio de lo anterior, el/la ESI debe programar actividades de difusión de esta Política al interior del SERVICIO y coordinar 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 Seguridad y Privacidad 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 funcionarios(as) que se integren al SERVICIO.

9. VIGENCIA Y REVISIÓN

La presente política será evaluada y revisada, al menos, una vez al año por el o la ESI, o cuando el CDS lo requiera, para asegurar su continuidad e idoneidad, considerando cambios externos o internos que puedan afectarla.

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.

10. SANCIONES POR INCUMPLIMIENTO

Las sanciones ante el incumplimiento de la presente política, así como la de cualquier otra política, procedimiento o instructivo, asociados al SGSPI, se regulará en el **PR-38-SGSPI Procedimiento sanciones por incumplimiento de las políticas y normativa asociadas a la seguridad de la información**.