I. MUNICIPALIDAD DE CERRILLOS
SECRETARIA MUNICIPAL

001276

DECRETO EXENTO N°202 / / 2024

Cerrillos, 13 AGO 2024

V I S T O S:

La Nonagésima Primera Sesión Ordinaria del Concejo Municipal, de fecha 4 de enero de 2024; el Certificado N°007/2024 de la Secretaria Municipal (s); la Providencia Alcaldicia N°100/478/2024; el Ordinario N°700/244/2024 de la Dirección de Tránsito y Transporte Público; SUBD IA Ordinario N°89 del Servicio de Registro Civil e Identificación; las facultades que me confiere D.F.L. N°1 del Ministerio del Interior, Subsecretaría de Desarrollo Regional y Administrativo, Fija Texto Refundido, Coordinado y Sistematizado de la Ley N°18.695, Orgánica Constitucional de Municipalidades.

C O N S I D E R A N D O:

El acuerdo adoptado en la Nonagésima Primera Sesión Ordinaria del Concejo Municipal, realizada con fecha 4 de enero de 2024.

D E C R E T O:

1. Apruébase el **"CONVENIO DE ADHESION CONECTIVIDAD Y PRESTACION DE SERVICIOS DE INFORMACION DIRECCION DE TRANSITO, JUZGADO POLICIA LOCAL"**, de fecha 17 de julio de 2024, suscrito con el **Servicio de Registro Civil e Identificación**, representado por su Director don **Omar Morales Marquez** y la Ilustre Municipalidad de Cerrillos, con el objetivo de que la municipalidad obtenga información del SERVICIO, bajo la modalidad de conexión a su red corporativa, para los efectos de acceder a la emisión de los documentos electrónicos y consultas a la base de datos que a continuación se indican, los que serán utilizados dentro del marco de las competencias de la municipalidad, cuyas condiciones para su ejecución y sus limitaciones, se establecen en el convenio que por este acto se aprueba:

LA MUNICIPALIDAD podrá acceder a la red de **EL SERVICIO** durante doce (12) horas al día, seis (6) días a la semana, a través de ocho (8) 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:

• Tres (5) 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 de **EL 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.

• Tres (3) puestos de trabajo estarán ubicados en el Juzgado de Policía Local, desde el cual sólo se podrá acceder a:

a. Emisión de Documentos Electrónicos
El/Los Juzgado/s de Policía Local de **LA MUNICIPALIDAD** podrá emitir los siguientes 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.

b. Consultas a la Base de Datos
El/Los Juzgado/s de Policía Local de LA MUNICIPALIDAD podrá acceder a la consulta de la base de datos de EL 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).

I. MUNICIPALIDAD DE CERRILLOS
SECRETARIA MUNICIPAL

001276

DECRETO EXENTO Nº202 / / 2024

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.

2. El texto del referido Convenio que por este acto se aprueba, se adjunta y forman parte integrante del presente decreto, el cual consta de 22 cláusulas.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE Y ARCHÍVESE

I. MUNICIPALIDAD DE CERRILLOS SECRETARIA MUNICIPAL

TAMARA GOMEZ TABILO
Secretaria Municipal(s)

I. MUNICIPALIDAD DE CERRILLOS ALCALDESA

LORENA FACUSE ROJAS
Alcaldesa

LFR/TGT/aaa
Distribución:
Archivo Virtual "Decretos Correlativos"
Servicio de Registro Civil e Identificación
Juzgado de Policía Local de Cerrillos
Dirección de Tránsito y Transporte Publico
Página Web.

I. MUNICIPALIDAD DE CERRILLOS
SECRETARIA MUNICIPAL

CERTIFICADO N°007/2024

Cerrillos, 23 de enero de 2024.

La Secretaria Municipal (s) que suscribe, certifica que en la Nonagésima Primera Sesión Ordinaria del Concejo Municipal, realizada con fecha 4 de enero del 2024 y con la asistencia de todos sus miembros, por unanimidad, la suscripción del "**CONVENIO DE ADHESION CONECTIVIDAD Y PRESTACION DE SERVICIOS DE INFORMACION DIRECCION DE TRANSITO Y JUZGADO DE POLICIA LOCAL"**, con el Servicio de Registro Civil e Identificación.-

El presente certificado se extiende en virtud del artículo 49 Título VI del Reglamento de Funcionamiento del Concejo Municipal, sancionado por Decreto Exento N°202/1542/2017 y sus modificaciones posteriores, para elaborar el decreto alcaldicio respectivo.

I. MUNICIPALIDAD DE CERRILLOS
SECRETARIA MUNICIPAL

TAMARA GOMEZ TABILO
Secretaria Municipal(s)

T.G.T.

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

En Santiago de Chile, a 17 JUL 2024, entre el Servicio de Registro Civil e Identificación, en adelante **EL SERVICIO**, RUT Nº[illegible] representado por su Director Nacional , don Omar Morales Márquez, RUN N[illegible] ambos domiciliados en [illegible], comuna de [illegible] y la Ilustre Municipalidad de Cerrillos, en adelante **LA MUNICIPALIDAD**, RUT Nº[illegible] representada por su Alcaldesa, doña Lorena Facuse Rojas, RUN N°[illegible] ambos domiciliados en Piloto Lazo N°120,Comuna de Cerrillos, se ha acordado lo siguiente:

PRIMERO: 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; 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; en la Ley N°19.477, de 1996, del Ministerio de Justicia, que Aprueba Ley Orgánica del Servicio de Registro Civil e Identificación; en el Decreto Ley N°645, de 1925, del Ministerio de Justicia, Sobre el Registro General de Condenas; en 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; en 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; Ley N°18.287, de 1984, del Ministerio de Justica, que Establece Procedimiento ante los Juzgados de Policía Local; en el Decreto con Fuerza de Ley N°1, de 2009, del Ministerio de Transportes y Telecomunicaciones y Ministerio de Justicia, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley de Tránsito; en 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; en el Decreto Supremo Nº61, de 2008, del Ministerio de Justicia, que Aprueba Reglamento del Registro de Multas de Tránsito No Pagadas; y en la Ley Nº19.628, de 1999, del Ministerio

Secretaría General de la Presidencia, sobre Protección a la Vida Privada; y atendido los Principios de Colaboración y Gratuidad que informa las relaciones entre los distintos entes que conforman la Administración del Estado.

SEGUNDO: Objeto

El presente Convenio de Adhesión tiene por finalidad que **LA MUNICIPALIDAD** obtenga información de **EL SERVICIO**, bajo la modalidad de conexión a su red corporativa, para los efectos de acceder a la emisión de los documentos electrónicos y consultas a la base de datos que a continuación se indican, los que serán utilizados dentro del marco de las competencias de **LA MUNICIPALIDAD**.

TERCERO: Requisitos para la Conectividad

La conexión de cada puesto de trabajo a la red corporativa de **EL SERVICIO** 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 cualquier navegador con Windows hasta la versión 10, 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 de los documentos electrónicos que se detallan en la cláusula CUARTO, serán de cargo de **LA MUNICIPALIDAD**.

No obstante, lo anterior, **EL SERVICIO** podrá adoptar en el futuro otro mecanismo de conectividad, de acuerdo a sus necesidades o en virtud de requerimientos generales de modernización del Estado tales como gobierno digital o electrónico, o bien por mandatos técnicos y legales de la autoridad competente, y previa coordinación con **LA MUNICIPALIDAD**.

CUARTO: Acceso y Puestos de Trabajo

LA MUNICIPALIDAD podrá acceder a la red de **EL SERVICIO** durante doce (12) horas al día, seis (6) días a la semana, a través de ocho (8) 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:

- Tres (5) 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 de **EL 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.

- Tres (3) puestos de trabajo estarán ubicados en el Juzgado de Policía Local, desde el cual sólo se podrá acceder a:

  a. **Emisión de Documentos Electrónicos**
  El/Los Juzgado/s de Policía Local de **LA MUNICIPALIDAD** podrá emitir los siguientes 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.

b. <u>Consultas a la Base de Datos</u>

El/Los Juzgado/s de Policía Local de **LA MUNICIPALIDAD** podrá acceder a la consulta de la base de datos de **EL 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.

<u>QUINTO</u>: Cuentas de acceso

El Coordinador/a designado/a por **LA MUNICIPALIDAD**, a través del Formulario de Solicitud de Cuentas Computacionales definido por **EL SERVICIO** para tales efectos, solicitará a la Plataforma Usuarios de **EL SERVICIO**, a través del correo electrónico <u>cuentas@registrocivil.gob.cl</u>, la creación de las cuentas de los usuarios habilitadas para efectos de conectarse a la red corporativa de **EL SERVICIO**.

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.

Dichas cuentas computacionales, tendrán el carácter de secretas, personales, indelegables e intransferibles, y su mal uso acarreará la responsabilidad administrativa que corresponde a todo funcionario municipal, la cual deberá perseguirse y hacerse efectiva por **LA MUNICIPALIDAD**, de conformidad a 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 haya lugar.

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

Asimismo, **LA MUNICIPALIDAD** estará obligado a comunicar por escrito a **EL SERVICIO**, el cambio de él/los funcionario/s designado/s para los efectos antes señalados, a través del Formulario individualizado precedentemente.

El incumplimiento de comunicar a el/la coordinador/a de **EL SERVICIO** la designación o el cambio de el/la funcionario/a designado por **LA MUNICIPALIDAD**, facultará a **EL SERVICIO** para poner término en forma inmediata al presente Convenio de Adhesión.

SEXTO: 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, el/la Coordinador/a de **LA MUNICIPALIDAD** deberá enviar copia de dicha instrucción y/o de los respectivos contratos a el/la Coordinador/a de **EL SERVICIO.**

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

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

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

SÉPTIMO: Precio

Los valores que **LA MUNICIPALIDAD** deberá pagar por la prestación de servicios que se establecen en el presente convenio, corresponden solo 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.

OCTAVO: 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 mediante transferencia electrónica 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 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.

NOVENO: Operatividad del sistema

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 sistema que da cuenta el presente Convenio de Adhesión.

DÉCIMO: 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 de **EL SERVICIO**, evento en el cual **LA MUNICIPALIDAD** deberá indicar los fines, el medio de difusión y el destinatario. Su no cumplimiento será causal de término del convenio contemplado en la Cláusula DÉCIMO QUINTO.

UNDÉCIMO: Propiedad y exclusividad de los sistemas de información

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

DUODÉCIMO: Continuidad del servicio

Toda mantención, readecuación o interrupción de la operación del sistema, programada o no, deberá ser comunicada oportunamente, por parte de el/la Coordinador/a de **EL SERVICIO** mediante correo electrónico a el/la Coordinador/a definido 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 sistema, que tengan su origen en labores de mantención o readecuación; o, caso fortuito o fuerza mayor.

DÉCIMO TERCERO: Daños y perjuicios

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.

DÉCIMO CUARTO: 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 Alcalde de **LA MUNICIPALIDAD** o al Director Nacional de **EL SERVICIO**, según sea el caso.

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

DÉCIMO QUINTO: 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**, y/o el/la funcionario/a 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 a **EL SERVICIO**, el cambio de él o los funcionarios designados para los efectos de conectarse a la red de **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 el Coordinador/a designado en la cláusula DÉCIMO SÉPTIMO, no de aviso de este hecho a **EL 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.

DÉCIMO SEXTO: De los saldos insolutos

En caso de que se registren saldos insolutos ya sea respecto del concepto de emisión de certificados valorados como por facturas emitidas al mes de noviembre del año 2020 por concepto de habilitación y/o conectividad mensual, de conformidad a lo establecido en la Resolución Exenta N°2242 de fecha 23 de septiembre de 1999, **LA MUNICIPALIDAD** se obliga expresamente a regularizar dichos saldos insolutos en un plazo de hasta un (1) año, una vez completamente tramitado el presente convenio. Lo anterior, en atención a que para efectos de proceder a la primera renovación en los términos señalados en la cláusula DÉCIMO CUARTO Duración y vigencia del presente instrumento, será requisito esencial que **LA MUNICIPALIDAD** acredite el pago total de las deudas ya indicadas.

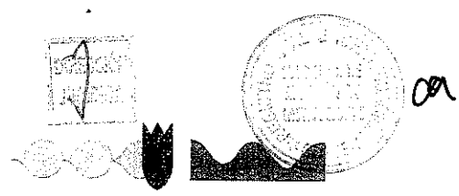
DÉCIMO SÉPTIMO: Coordinadores/as

Con el objeto de velar por el fiel cumplimiento del presente Convenio, cada una de las partes designará un/a coordinador/a:

- Por **EL SERVICIO**:
  El Director Regional de la Dirección Regional Metropolitana de **EL SERVICIO**, don Jorge Zuñiga Cabezas, correo electrónico jzunigac@registrocivil.gob.cl, fono (56 -2) 261-14302 o quien le subrogue en el cargo.

- Por **LA MUNICIPALIDAD**:
  La Directora de Tránsito y Transporte Público de **LA MUNICIPALIDAD**, doña Marisol Varas Cisternas, correo electrónico mvaras@mcerrillos.cl, fono (56-2) 33278159 o quien le subrogue en el cargo.

En el evento de modificarse la designación de el/la o los/as Coordinadores/as, se deberá dar aviso, 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.



DÉCIMO OCTAVO: 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.

DÉCIMO NOVENO: 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 de **EL SERVICIO** y del Alcalde de **LA MUNICIPALIDAD**.

VIGESIMO: Deja sin efecto

Por este acto, las partes acuerdan dejar sin efecto el Convenio de Conectividad y Prestación de Servicios entre el Servicio de Registro Civil e Identificación y la Ilustre Municipalidad de Cerrillos, suscrito el 22 de agosto de 2007 y aprobado mediante Resolución Exenta N°2620, de fecha 25 de septiembre de 2007, de **EL SERVICIO**.

VIGÉSIMO PRIMERO: 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.

VIGÉSIMO SEGUNDO: Personerías

La personería de don Omar Morales Márquez para actuar a nombre y en representación de **EL SERVICIO** consta en Decreto Supremo N°140, de 14 de diciembre de 2022, del Ministerio de Justicia y Derechos Humanos, que nombra al Director Nacional del Servicio de Registro Civil e Identificación.

La personería de doña Lorena Facuse Rojas, para actuar a nombre y en representación de **LA MUNICIPALIDAD**, consta de Acta de Proclamación de fecha 22 de junio de 2021, del Primer Tribunal Electoral, Región Metropolitana a Fojas N°1293 y Fojas N°1294, Rol 8760-2021.

OMAR MORALES MÁRQUEZ
DIRECTOR NACIONAL
SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN

LORENA FACUSE ROJAS
ALCALDESA
ILUSTRE MUNICIPALIDAD DE CERRILLOS

LCS / AMC / DTB

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 Juridico (S)

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

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
		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".	

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.

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

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.

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

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

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.

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.**

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)

UNIDAD DE GESTIÓN ESTRATÉGICA
Avda. Libertador Bdo. O"Higgins N°1449, Torre 4, piso 20
(+56 2) 261 14757

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

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.

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.

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.

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)	Claus Cisternas 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

Departamento de Gestión Institucional, Transparencia, Ciudadanía y Patrimonio
Avda. Libertador Bdo. O"Higgins N°1449, Torre 4, Piso 21
(+56 2) 261 14187.

Publico Uso Interno

REVISIONES DEL PROCEDIMIENTO

Nº 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°263, 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.

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 SRCel 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 SRCel 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 SRCel, 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.

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
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
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.

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.