CONVENIO DE CONECTIVIDAD Y PRESTACIÓN DE SERVICIOS DE ENTREGA DE CERTIFICADOS
ENTRE
EL SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN Y
LA ILUSTRE MUNICIPALIDAD DE RÍO BUENO

En Santiago de Chile, a 3 SET. 2020, entre el Servicio de Registro Civil e Identificación, en adelante **EL SERVICIO**, RUT N°61.002.000-3, representado por su Director Nacional, don Jorge Álvarez Vásquez, RUN N°9.603.153-K, ambos domiciliados en Avenida Libertador Bernardo O'Higgins N°1449, Edificio Santiago Downtown, Torre 4, Piso 21, comuna de Santiago y la Ilustre Municipalidad de Rio Bueno, en adelante **LA MUNICIPALIDAD**, RUT N°69.201.000-0, representada para estos efectos por su Alcalde, don Luis Reyes Álvarez, RUN N°8.818.022-4, ambos domiciliados en Comercio N°603, comuna de Río Bueno, 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, que establece el texto Refundido, Coordinado y Sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N°19.477, Orgánica del Servicio de Registro Civil e Identificación; la Ley N°19.880, que Establece Bases de los Procedimientos Administrativos que Rigen Los Actos de los Órganos de la Administración del Estado; el Decreto Ley N°645, de 1925, sobre el Registro General de Condenas; el Decreto N°64, de 1960, 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; la Ley N°18.287, que Establece Procedimientos ante los Juzgados de Policía Local; la Ley N°18.290, de Tránsito; Ley N°18.695, Orgánica Constitucional de Municipalidades; el Decreto N°1.111, de 1984, que Aprueba Reglamento de Registro de Vehículos Motorizados; el Decreto Supremo N°61, de 2008, que Aprueba el Reglamento del Registro de Multas de Tránsito No Pagadas y la Ley N°19.628, Sobre Protección de la Vida Privada.

SEGUNDO: Objeto

El presente Convenio tiene por finalidad 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 certificados 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 laser blanco negro o color, emulación HP PCL 5.0 o 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. Solo compatible con Internet Explorer.
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 correspondientes certificados, 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 un (01) puesto de trabajo, con un máximo de tres (3) cuentas de acceso para cada puesto de trabajo, con el objeto de emitir los certificados electrónicos que se señalan en el presente Convenio:

- Un (01) puesto de trabajo que estará ubicado 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:

  a) 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.
  b) 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 distintas Municipalidades.
  c) Certificado de Multas del Tránsito no Pagadas.

DIRECCIÓN NACIONAL

CAUTIVO CAUTIVO

QUINTO: 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 Unidad de Atención de Instituciones de **EL SERVICIO**, a través del correo electrónico convenios@srcei.cl, la creación de las cuentas de los usuarios habilitadas para efectos de conectarse a la Red corporativa de **EL SERVICIO**. Estas cuentas podrán tener diferentes privilegios, de ser así requerido.

En caso 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 OCTAVO

Dichas cuentas computacionales, tendrán el carácter de secretas, personales, indelegables e intransferibles, y su mal uso acarreara 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.

Asimismo, **LA MUNICIPALIDAD** estará obligada 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 SERVICIO estará facultado para efectuar la supervisión, control y auditoría en materia de cuentas de acceso que digan relación con el objeto del presente convenio. Para lo anterior, **LA MUNICIPALIDAD** deberá proporcionar todas las facilidades destinadas a la ejecución de las acciones de supervisión y auditoría que **El SERVICIO** deba ejecutar

El incumplimiento de no comunicar al/la coordinador/a de **EL SERVICIO** la designación o el cambio del/la funcionario/a designado por **LA MUNICIPALIDAD**, facultará a **EL SERVICIO** para poner término en forma inmediata al presente Convenio.

SEXTO: Limitaciones en el uso de la Información

LA MUNICIPALIDAD se obliga a utilizar la información proporcionada por **EL SERVICIO**, 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, que estrictamente tengan la obligación de conocerla evitando el acceso a terceros no autorizados.

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, respecto a la imposibilidad absoluta de copiarla, total o parcialmente, revelar, publicar, difundir, vender, ceder, copiar, reproducir, interferir, interceptar, alterar, modificar, dañar, inutilizar, destruir, ya sea durante la vigencia del convenio como después de su término.

En consecuencia, **LA MUNICIPALIDAD** deberá velar por el cumplimento de la Ley N°19.628, sobre Protección de la Vida Privada.

SÉPTIMO: Precio

Los valores que **LA MUNICIPALIDAD** deberá pagar por la conectividad y prestación de servicios que se establecen en el presente Convenio, son los siguientes:

1. Por concepto de habilitacion y acceso
   Los valores asociados a este concepto, se encuentran establecidos por Resolución Exenta N°2242, que Establece Valores por la Prestación de los Servicios Computacionales Denominados "Conexiones a la Red Corporativa para Organismos de la Administración del Estado" de fecha 23 de Septiembre de 1999, del Servicio de Registro Civil e Identificación, donde **LA MUNICIPALIDAD**, deberá pagar por los siguientes servicios

   - Valor de Habilitación de Acceso y Configuración de Equipos: 20 UF
     (Hasta tres (3) Puestos de Trabajo)
   - Valor de Configuración por cada Puesto de Trabajo Adicional: 3 UF
   - Valor Mensual de Conectividad por cada Puesto de Trabajo: 5 UF
   - Valor de Reposición por cada Puesto de Trabajo conectado: 2 UF

2. Por concepto de emisión de certificados:
   Los valores correspondientes a los certificados emitidos que tengan el carácter de valorados, serán aquellos fijados por Decreto del Ministerio de Justicia.

OCTAVO: Forma y oportunidad de pago

I. Por concepto de habilitacion y acceso:
   La factura correspondiente al Valor de Habilitación de Acceso y Configuración de Equipos, se emitirá y enviará a **LA MUNICIPALIDAD** con posterioridad a la fecha de la total tramitación del acto administrativo que apruebe el presente convenio, y una vez ejecutada dicha habilitación y acceso.

Por otra parte, la factura correspondiente al Valor Mensual de Conectividad por cada Puesto de Trabajo, se emitirá y enviará a **LA MUNICIPALIDAD** posteriormente al mes de la prestación del servicio, conjuntamente, con el Valor de Reposición por cada Puesto de Trabajo conectado si correspondiere, siendo de exclusiva responsabilidad de ésta dar cumplimiento a lo establecido en la Ley N°19.983, que Regula la Transferencia y Otorgamiento de Mérito Ejecutivo a Copia de la Factura.

Las facturas emitidas por el Departamento de Finanzas y Contabilidad del Nivel Central de **EL SERVICIO**, deberán pagarse por **LA MUNICIPALIDAD** mediante alguna de las siguientes modalidades:

1. De preferencia, transferencia electrónica en la Cuenta Corriente N°901750-0 RUT N°61.002.000-3 del Banco Estado de **EL SERVICIO**, transacción que deberá precisar a lo menos el número de la factura a pagar, y debera ser informada a **EL SERVICIO** vía correo electrónico a depositos@srcei.cl con copia al correo convenios@srcei.cl; o bien,

2. Cheque nominativo y cruzado, a nombre del Servicio de Registro Civil e Identificación, el cual deberá ser depositado en la Cuenta Corriente N°901750-0, o bien puede ser cancelado directamente en la Unidad de Tesorería de **EL SERVICIO**.

Todos los pagos se realizarán en pesos chilenos, una vez efectuada la conversión según el valor vigente para la Unidad de Fomento (UF) del último día del mes al que corresponde el servicio prestado. A todos los precios expresados deberá adicionárseles el Impuesto al Valor Agregado (IVA).

LA MUNICIPALIDAD se obliga a pagar la correspondiente facturación, dentro del plazo de treinta (30) días corridos contados desde la fecha de recepción de la correspondiente factura electrónica.

II. Por concepto de emisión de certificados:
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 de Los Ríos, 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 cheque nominativo y cruzado a nombre del Servicio de Registro Civil e Identificación, el cual deberá ser entregado en la Unidad de Finanzas de la Dirección Regional de Los Ríos,de **EL SERVICIO**.

CALIDAD CALIDAD

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.

DÉCIMO: Uso publicitario

Todo uso publicitario que **LA MUNICIPALIDAD** quisiera hacer respecto de la entrega de datos objeto del presente Convenio 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 termino del convenio contemplado en la Cláusula DECIMO QUINTO.

UNDÉCIMO: Propiedad y exclusividad de los sistemas de información

Para los efectos del presente Convenio se considerará propiedad de **EL SERVICIO**, sin limitación alguna, los registros, diseños de hardware, redes y software, diagramas de flujo de programas y sistemas, estructuras de archivos, listados de código fuente u objeto, programas de computación, arquitectura de hardware, documentación y otros informes de 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.

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, o perjuicios 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.

DÉCIMO CUARTO: Duración y vigencia

El presente convenio entrará en vigencia a partir de la fecha de la total tramitación del acto administrativo que lo apruebe, y tendrá un plazo de duración de un (1) año, el que se renovará automáticamente por períodos iguales y sucesivos, por un máximo de (4) períodos, salvo que alguna de las partes manifieste a la otra su voluntad de poner término al convenio a través de un aviso, dirigido al 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, en los siguientes casos:

1. Que, **LA MUNICIPALIDAD** no mantenga 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, **LA MUNICIPALIDAD** retrase el pago de dos (2) o más facturas sean o no consecutivas, por el valor de los servicios de información prestados, de acuerdo a lo establecido en la cláusula respectiva.
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: 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**:
  La Directora Regional (S) de Los Ríos de **EL SERVICIO**, doña Pilar Camino Bucarey, correo electrónico ncamino@registrocivil.gob.cl, fono (56-63) 2672502, o quien le subrogue en el cargo.

- Por **LA MUNICIPALIDAD**:
  El Director de Tránsito de **LA MUNICIPALIDAD**, don Miguel Cereceda Asencio, correo electrónico transitorbnc@muniriobueno.cl, fono (56-64) 2340413, o quien le subrogue en el cargo.

DIRECCIÓN NACIONAL

CALIDAD CALIDAD

En el evento de modificarse la designación de el/la o los/as Coordinadores/as, se debera 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 SÉPTIMO: Copias

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

DÉCIMO OCTAVO: Anexos

Las partes acuerdan que en el evento de ser necesario suscribir algun Anexo éste se entenderá formar parte integrante del presente Convenio, lo que debera ser aprobado mediante Resolución del Director Nacional de **EL SERVICIO**.

DÉCIMO NOVENO: Solución de conflictos

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

VIGÉSIMO: Personerías

La personería de don Jorge Álvarez Vásquez, para actuar a nombre y en representación de **EL SERVICIO**, consta en el Decreto Supremo N°900, de fecha 03 de octubre de 2018, del Ministerio de Justicia y Derechos Humanos.

La personería de don Luis Reyes Álvarez, para actuar a nombre y en representación de **LA MUNICIPALIDAD**, consta en Decreto Alcaldicio N°2.779, de fecha 06 de diciembre de 2016, de la Ilustre Municipalidad de Río Bueno.

JORGE ÁLVAREZ VÁSQUEZ
DIRECTOR NACIONAL
SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN

LUIS REYES ÁLVAREZ
ALCALDE
ILUSTRE MUNICIPALIDAD DE RÍO BUENO

ARC / ESG / SML / JNS / AMC

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

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

V°B° Ingrid Reyes Constant – Subdirectora Jurídica

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

Control de Cambios

Nº Versión	Fecha	Motivo de la revisión	Páginas elaboradas o modificadas
0 (cero)	31/10/2012	Elaboración de acuerdo a los lineamientos del Sistema de Seguridad de la Información (SSI) y los requisitos de las normas NCh-ISO 27001.2013	Todas
1 (uno)	24/08/2015	Se ajusta el documento en los Principios de la Política	Todas
2 (dos)	20/11/2017	Se revisa número de versión de política Se valida el contenido de la política y se actualizan los contenidos	Todas
3 (tres)	26/04/2018	Se revisa número de versión de política Se valida el contenido de la política y se actualizan los contenidos	Todas
4 (cuatro)	31/07/2019	Se revisa número de versión de política Se valida el contenido de la política y se actualizan los contenidos	Todas

I. OBJETIVO

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

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

II. ALCANCE

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

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

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

III. ROLES Y RESPONSABILIDADES

- Directoría Nacional:
  - Aprobar y difundir la presente política al interior del SRCeI.
  - Proveer los recursos necesarios para la implementación de la presente política.
- Jefe de Riesgo Tecnológico y Seguridad TI:
  - Informar sobre aquellas modificaciones que sean necesarias incorporar a la presente política.
  - Sugerir las modificaciones que sean necesarias de considerar, en la revisión anual de la presente política.
  - Visar la presente política.
- Subdirector de Estudios y Desarrollo:
  - Revisar y aprobar la presente política.
  - Proveer los recursos necesarios para la implementación de la presente política.
  - Velar por el cumplimiento de la presente política.
- Subdirector Jurídico:
  - Revisar y visar la presente política.

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

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

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

IV. DEFINICIONES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

V. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

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

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

VI. DIFUSIÓN

La presente política deberá ser difundida a los funcionarios de planta y a contrata del 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.
Para estos efectos, el documento estará disponible y publicado en el sitio web del Sistema de Gestión Integral de Calidad del SRCeI, específicamente, en la Documentación del Proceso de la Subdirección de Estudios y Desarrollo, cuya URL es la siguiente http://calidad.srcei.cl/sgic/

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ELABORADO POR	REVISADO POR	APROBADO POR
Gonzalo Navarrete Parra Jefe de Riesgo Tecnológico y Seguridad TI	Sergio Mondaca Leiva Subdirector de Estudios y Desarrollo (S)	Jorge Álvarez Vásquez Director Nacional

V°B° Ingrid Reyes – Subdirectora Jurídica

HISTORIAL DE VERSIONES

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

1. DECLARACIÓN INSTITUCIONAL.

El Servicio de Registro Civil e Identificación (en adelante, SRCeI), se compromete a gestionar la Seguridad de la Información para lograr niveles adecuados de confidencialidad, integridad y disponibilidad de los activos de información que la institución considere relevantes. Para ello, desarrollará un trabajo paulatino de implementación de un Sistema de Seguridad de la Información (en adelante, SSI) basado en la Norma Chilena NCh ISO 27001, realizando lineamientos y unificando criterios en aspectos de seguridad, con el objetivo de preservar dichos activos de información, respecto a:

Confidencialidad: El SRCeI deberá velar porque se apliquen los controles necesarios para resguardar a 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.

Integridad: El SRCeI deberá velar porque se apliquen los controles necesarios para resguardar a 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.

Disponibilidad: El SRCeI deberá velar porque se apliquen los controles necesarios para resguardar a 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.

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

2. OBJETIVOS.

2.1. Proteger aquellos Activos de Información que tengan una relevancia para la Institución identificados a través del Inventario de Activos de Información, para asegurar su confidencialidad, integridad y disponibilidad, a objeto de mantener y asegurar la continuidad operativa del SRCeI.

2.2. Establecer los mecanismos para la clasificación e identificación de activos de información relevantes para la Institución para su posterior evaluación de riesgo y establecimiento de medidas de mitigación.

2.3. Incorporar en forma paulatina la evaluación de riesgo de los activos de información al Proceso de Gestión de Riesgo institucional.

2.4. Definir una estructura y un marco de políticas, procedimientos, instructivos entre otros estándares para gestionar la seguridad de la información en base a la Norma Chilena NCh ISO 27001.

2.5. Establecer los mecanismos de difusión, sensibilización y capacitación de la presente Política para el personal del SRCeI, a objeto que cuenten con las competencias en materias concernientes a la presente Política y a otras asociadas al Sistema de Seguridad de la Información y desarrollará una cultura institucional de la Ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.

2.6. Establecer los mecanismos de difusión para terceras partes, en especial lo referente a la confidencialidad de la información de la que tome conocimiento mientras dure el contrato o convenio, sus derechos y obligaciones en materia de seguridad de la información del Servicio y las consecuencias en caso de no cumplimiento, establecidos en los respectivos contratos o convenios.

2.7. Adherir a los lineamientos políticos del Estado de Chile en materia de **Ciberseguridad**, para alcanzar el objetivo de contar con un ciberespacio seguro.

2.8. Gestionar un entorno seguro de las redes y los sistemas de información a través del fortalecimiento de sus capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques.

3. ALCANCE.

El ámbito de aplicación de la Política de Seguridad de la Información contempla los dominios contenidos en la Norma Chilena NCh-ISO 27002:2013 que se enumeran a continuación, aplicados a los activos de información que la organización considera relevante resguardar, y que están asociados a los procesos de provisión de bienes y servicios que proporcionan los productos estratégicos de la Institución.

i) Políticas de Seguridad de la Información.
ii) Organización de la seguridad de la información.
iii) Seguridad de Recursos Humanos.
iv) Administración de Activos.
v) Control de Acceso.
vi) Criptografía.
vii) Seguridad Física y Ambiental.

viii) Seguridad de las Operaciones.

ix) Seguridad en las Comunicaciones.

x) Adquisición, desarrollo y mantenimiento de sistemas.

xi) Relación con los proveedores.

xii) Administración de incidentes de seguridad de la información.

xiii) Aspectos de la seguridad de la información de la gestión de la continuidad comercial.

xiv) Cumplimiento.

En cuanto a los controles a implementar relacionados con los dominios previamente señalados, se determinarán en base a un análisis de los riesgos y amenazas a los que estén expuestos los activos de información críticos, por parte del Encargado de Seguridad de la Información, Encargado de Ciberseguridad, Comité Operativo de Seguridad de la Información y/o las jefaturas y/o dueños de activos o procesos.

Con todo, la presente Política deberá ser aplicada y cumplida por **todos los funcionarios** de planta y a contrata, así como 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.

4. ROLES Y RESPONSABILIDADES.

4.1. Estructura del Sistema de Seguridad de la Información.

El SRCel contará con una estructura funcional del Sistema de Seguridad de la Información que considera:

Rol	Responsabilidad
Director/a Nacional	(a) Proveer los medios para la implementación de esta Política de Seguridad de la Información. (b) Aprobar las versiones actualizadas de esta Política.
Comité Directivo de Seguridad de la Información (CDS).	(a) Revisar, aprobar y difundir las políticas de seguridad. (b) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes de seguridad. (c) Promover la difusión y apoyo a la Seguridad de la Información.

Rol	Responsabilidad
Comité Operativo de Seguridad de la Información (COS).	(a) Proponer al Comité Directivo de Seguridad de la Información del Servicio de Registro Civil e Identificación, nuevas políticas de seguridad de la información. (b) Supervisar la implementación de procedimientos e instructivos que tengan lineamientos desde las políticas de seguridad de la información. (c) Identificar los riesgos a los cuales se encuentran expuestos los activos de información, definir estrategias y proponer al Comité Directivo de Seguridad de la Información, un Plan para su tratamiento y mitigación.
Encargado/a de Seguridad de la Información (ESI)	(a) Asesorar, coordinar y apoyar a la institución en materias relativas a la Seguridad de la Información. (b) Difundir y sensibilizar respecto de la Seguridad de la Información a los funcionarios/as de la institución. (c) Gestionar los riesgos asociados a los activos de información del Servicio.
Jefatura Unidad Control de Riesgos y Seguridad	(a) Generar la definición y materialización de los planes de corto, mediano y largo plazo relativos a la seguridad de la información.
Encargado/a de Ciberseguridad	(a) Gestionar la seguridad informática del Servicio y los riesgos asociados a la Ciberseguridad.
Oficial de Seguridad TI	(a) Prestar asesoría técnica especializada al Encargado/a de Seguridad de la Información, al Subdirector/a de Estudios y Desarrollo y al Director/a Nacional en las materias relativas a la seguridad de los Sistemas Informáticos y Documentos Electrónicos.
Encargados/as de Seguridad de la Información Regionales	(a) Asesorar al Director/a Regional. Respecto de alcances, de las Políticas y normas internas asociadas a la Seguridad de la Información, así como a todos los funcionarios y funcionarias de la región. Así como también informar cualquier acto anómalo detectado sobre el tratamiento de los activos de información.

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 de la Institución, o que tengan acceso al uso de las tecnologías de la información y sus actividades en Internet; dar cumplimiento a la presente Política y a otras políticas, procedimientos o instructivos asociados al Sistema de Seguridad de la Información.

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

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

Las **Subdirección de Estudios y Desarrollo**, debe velar porque aquellos acuerdos o convenios relacionados con los activos de información del SRCeI den cumplimiento a la presente Política y otras políticas, procedimientos o instructivos asociados al Sistema de Seguridad de la Información.

La **Unidad de Atención a Instituciones**, debe asegurar que los acuerdos o convenios mencionados en el párrafo anterior, incluyan cláusulas de confidencialidad, integridad y disponibilidad, como también sobre sanciones por incumplimiento de estas, respectivos de la información y de la ejecución de los mismos.

5. DEFINICIONES

Concepto	Descripción
Activos de Información	Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización de información de valor para la organización.
Ciberseguridad	Es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.
Confidencialidad	Es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados.

Concepto	Descripción
Disponibilidad	Cualidad o condición de la información de encontrarse a disposicion de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones
Incidente de Seguridad	Se refiere a la identificación y materialización de una situación detectada respecto de fallas en sistemas, controles o incumplimiento de normativas asociadas a la seguridad de la información, que comprometan la continuidad operacional del Servicio
Integridad	Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
Inventario de Activos de Información	Activos de información que representan algún valor para la empresa y que quedan dentro del alcance del SGSI
Proceso	Conjunto de actividades planificadas que implican la participación de un número de personas y de recursos materiales coordinados para conseguir un objetivo previamente identificado
Proceso de Gestión de Riesgo Institucional	Proceso estructurado, consistente y continuo implementado a través de toda la organización para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el poder alcanzar el logro de sus objetivos
Sistema de Seguridad de la Información	Conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización.

6. INCUMPLIMIENTOS DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

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

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

7. PERIODICIDAD DE EVALUACION Y REVISIÓN

La presente política será evaluada y revisada al menos una vez al año por el **Encargado de Seguridad de la Información**, o cuando el Comité Directivo de Seguridad 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:

- Cambios legales y/o normativos que puedan afectar la presente Política.
- Eventos de seguridad que afecten la Confidencialidad, Integridad o Disponibilidad de los activos de información.

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

8. DIFUSIÓN

El SRCeI, mantendrá a disposición de los funcionarios/as, la versión actualizada de la presente política. Para estos efectos, el documento estará disponible y publicado en el sitio web del Sistema de Gestión Integral de Calidad del SRCeI, específicamente, en la Documentación del Proceso de la Subdirección de Estudios y Desarrollo, cuya URL es la siguiente http://calidad.srcei.cl/gsm/