POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Agosto 2025

Confidencial

Versión 1.3

Control de Cambios del Documento

Versión	Descripción	Fecha	Autor
0.1	Primera versión del documento	1/07/2005	C. Ríos
0.2	Modificación Responsables	26/08/2013	A. Riveros
0.3	Modificación Responsables	22/07/2014	S. Mercado
0.4	Actualización	22/10/2015	T. Riveros A. Carreño
0.5	Actualización Copias de Certificado SSL	01/11/2017	T. Riveros A. Carreño
0.6	Actualización e incorporación Protección Datos Personales	15/04/2019	R. Riveros R. Reveco
0.7	Actualización	15/06/2021	M. Robles A. Carreño
0.8	Revisión	03/08/2022	I. Infante
0.9	Revisión	07/08/2023	I. Infante
1.0	Agrega DPO	24/10/2023	A.Léniz
1.1	Borrador Política Privacidad y Protección de Datos Personales	20/11/2023	A.Léniz y R. Riveros
1.2	Documento a Revisión v1.2	23/11/2023	A.Léniz
1.3	Documento adecuado según Ley N° 21.719 Regula la Protección de Datos Personales y crea Agencia de Protección de Datos	05/08/2025	J.L. Morales

Tabla de contenido

GLOSARIO 5

1. Introducción 9

2. Objetivo 9

3. Alcance 9

4. Definiciones Generales 10

4.1 Obtención de los Datos 10

4.2 Recopilación y Uso de Datos 11

5. De la Información de los Certificados Digitales 11

6. Roles y responsabilidades en la Aplicación de la Política 12

6.1 Rol del Oficial de Protección de Datos (DPO) 12

6.2 Rol de los Responsables del Tratamiento de Datos 13

6.2.1 Cesión o Transferencia de Datos Personales (de Responsable a Responsable) 14

6.3 Rol de el o los encargados de Tratamiento de Datos 14

6.4 La Autoridad de Protección de Datos 15

6.5 Obligación de Reportar Brechas de Seguridad 17

6.6 Privacidad desde el Diseño y por Defecto y Evaluaciones de Impacto de Privacidad 17

6.7 Evaluaciones de Impacto de Privacidad (“PIA”). 18

6.8 La Agencia publicará una lista orientativa de los tipos de tratamiento que requerirán PIA. 18

6.9 Transferencia Internacional de Datos 19

7. Nuevas Bases de Licitud para Tratar Datos Personales 19

7.1 Consentimiento libre 19

7.2 Ejecución o cumplimiento de una obligación legal 20

7.3 Datos relativos a obligaciones de carácter económico, financiero, bancario o comercial 20

7.4 Celebración o ejecución de un contrato 20

7.5 Intereses legítimos 20

7.6 Formulación, ejercicio o defensa 20

8. Principios de la Protección de Datos 20

8.1 Principio de Licitud y Lealtad 20

8.2 Principio de Finalidad 21

8.3 Principio de Proporcionalidad 21

8.4 Principio de Responsabilidad 21
8.5 Principio de Transparencia: El aviso de Privacidad 22
8.6 Principio de Confidencialidad 22
9. Compromiso de Resguardo de información y Protección de Datos Personales de Titulares/Usuarios ... 22
9.1 Resguardo Información. 23
9.2 Directrices para los Colaboradores 24
9.3 Directrices de Sistemas y Aplicaciones 25
9.4 Difusión y Contacto 25
9.5 Cambios a la Política de Privacidad y Protección de Datos Personales 26
9.6 Derechos de los Interesados 26
9.7 Seguridad de Datos 26
9.8 Transferencia de Datos 26
9.9 Formación y Concienciación 27
9.10 Evaluación de Impacto de Protección de Datos (DPIA) 27
9.11 Auditorías y Revisión 27
10. Nuevo Catálogo de Derechos de los Titulares 27
10.1 Derecho de Acceso 27
10.2 Derecho de Rectificación 27
10.3 Derecho de Cancelación 27
10.4 Derecho de Oposición 28
10.5 Derecho de Oposición a Decisiones Individuales Automatizadas y Elaboración de Perfiles 28
10.6 Derecho de Bloqueo 28
10.7 Derecho de Portabilidad 28
10.8 Atención solicitudes de Titulares 29

GLOSARIO

PSC: Prestadora de Servicios de Certificación, entidad prestadora de servicios de certificación de Firmas Electrónicas de acuerdo con la Ley 19.799, Articulo 2°, letra c).

PSI: Política de Seguridad de la Información, es la declaración de alto nivel sobre la intención y la dirección de la Gerencia respecto al conjunto de medidas preventivas y reactivas de la organización y los sistemas tecnológicos que le permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los datos.

PKI: Public Key Infraestructure; Infraestructura de clave pública, es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital, y el no repudio de transacciones electrónica

CPS: (del inglés – Certification Practice Statement) conjunto de Prácticas de la PKI que declaran los términos y condiciones del servicio PKI que declara en forma pública.

CP: (del inglés – Certification Politics) políticas de certificación que usa el servicio PKI que declara en forma pública.

RA: Autoridad de Registro – unidad a cargo de identificar al solicitante de certificado, del inglés "Registration Authority" en PKI.

Oficiales RA: encargados de identificar al solicitante de certificado.

Oficial de Seguridad de la Información: Corresponde al rol encargado de coordinar, planear y promover las actividades que tengan que ver con la seguridad de la información de la empresa, con el objetivo de gestionar, detectar, administrar y mitigar los incidentes y problemas de seguridad que se presentan en la empresa, tales como intentos de intrusiones, faltas a las prácticas de seguridad definidas, infecciones con virus, falta de actualización de software, entre otros; velando por el cumplimiento de la legislación vigente en materia de Firma Electrónica con el fin de dar cumplimiento a los requisitos del Ministerio de Economía Fomento y Turismo, en el proceso de acreditación anual de la empresa.

SGSI: Sistema de Gestión de Seguridad de la información, corresponde al diseño, implantación y mantenimiento de los procesos y herramientas que permitan gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información y minimizando los riesgos de seguridad de la información.

Auditorías de seguridad: procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.

RFC: (del inglés Request For Change), proceso que se debe hacer frente a un cambio de un sistema.

ENISA: European Union Agency for Network and Information Security; Agencia de la Unión Europea para la Seguridad de las Redes y la Información.

NIST: National Institute of Standards and Technology, USA; Instituto Nacional de Estándares y Tecnología, EE.UU.

Ley Marco Ciberseguridad: tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones determinadas en su reglamento, respecto a instituciones que presten servicios calificados como esenciales y a aquellas que sean calificadas como operadores de importancia vital, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

Activo informático: toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.

Agencia Nacional de Ciberseguridad: servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, y coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad. Se conocerá en forma abreviada como ANCI.

Ciberataque: intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.

Ciberseguridad: preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.

Confidencialidad: propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.

Disponibilidad: propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.

Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT: centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.

Incidente de ciberseguridad: todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.

Integridad: propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.

Red y sistema informático: conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.

Resiliencia: capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.

Riesgo: posibilidad de ocurrencia de un incidente; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo.

Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

Dato personal: cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Datos Sensibles: datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Tratamiento de datos: cualquier operación o complejo de operaciones o procedimientos técnicos de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar

Titular de los datos: la persona natural a la que se refieren los datos de carácter personal.

Almacenamiento de datos: la conservación o custodia de datos en un registro o banco de datos.

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.

Responsable del registro o banco de datos: la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

Referencias a Leyes y Estándares:

- NCh-ISO IEC 27001:2013 y NCh-ISO IEC 27001:2020
- NCh-ISO IEC 27002:2022

- Ley 19 799: https://www.leychile.cl/Navegar?idNorma=196640&idParte=
- Decreto 181, Reglamento Ley 19.799: https://www.leychile.cl/Navegar?idNorma=201668
- NIST “Risk Management Guide for Information Technology Systems”:
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- ENISA: “Risk assessment for trust services providers”:
- https://www.enisa.europa.eu/publications/tsp2-risk
- Ley N° 21.719 Regula la Protección de Datos Personales y crea la Agencia de Protección de Datos Personales.
- Ley 21.663 Ley Marco de Ciberseguridad

1. Introducción

Certinet entiende la importancia estratégica de la protección y la privacidad de los datos personales de sus clientes, empleados y otras partes interesadas, y por ello se alinea con Ley chilena N° 21.719 que Regula la Protección de Datos Personales y crea la Agencia de Protección de Datos Personales, así como todas las actualizaciones que ella tenga.

Consistente con lo anterior, Certinet dispone de la tecnología y aplicaciones de clase mundial que cumplen con las normativas de la Unión Europea (UE) como es eIDas y GDPR en materia de protección de datos seguridad y privacidad.

Adicionalmente la dirección de la empresa ha definido el Rol de Oficial de Protección de Datos (DPO) quien enmarca su accionar y gobernanza por medio de esta Política de Protección de Datos y los correspondientes estándares que le son aplicables como es la normativa ISO 27701.

Este documento corresponde a una versión preliminar de la Política de Protección de Datos de Certinet la que deberá ser revisada y aprobada por el Directorio de la empresa para que pueda entrar en vigor. No obstante, se presenta para revisión, mejoras, previo a su formalización.

2. Objetivo

El objetivo de esta Política es establecer los principios, lineamientos y directrices que deben observarse para para garantizar la protección adecuada de los datos personales en cumplimiento de todas las leyes y regulaciones aplicables al tratamiento de los datos personales tanto de sus colaboradores, clientes y proveedores.

Lo anterior, a fin de velar por un tratamiento responsable de los datos personales de aquellas personas con las cuales la Organización mantiene o mantuvo un vínculo laboral o comercial.

3. Alcance

La presente Política de Protección de Datos personales es aplicable a la Organización, en calidad de responsable del tratamiento de datos personales, a sus Directivos, colaboradores directos e indirectos, como a todas aquellas terceras personas naturales o jurídicas a quienes se les transmita datos personales de los Titulares, en el marco de la Ley N° 21.719 que Regula la Protección de Datos Personales y crea la Agencia de Protección de Datos Personales. Por tanto, debe ser conocida y respetada por todos. La falta de cumplimiento de esta política puede dar lugar a medidas disciplinarias.

Sin perjuicio de lo anterior las obligaciones legales respecto a la confidencialidad de datos, de las personas que trabajan en su tratamiento o acceden a ellos de cualquier forma, no cesan por haber terminado sus actividades en el respectivo organismo.

4. Definiciones Generales

4.1 Obtención de los Datos

Certinet obtiene datos de sus usuarios, titulares dueños de sus datos personales, a través de mecanismos automatizados y mediante peticiones formales de inscripción, estos datos son ingresados por los propios Titulares/Usuarios voluntariamente. Se rige por la ley chilena, en particular por la ley N° 21.719 que Regula la Protección de Datos Personales y crea la Agencia de Protección de Datos Personales, asimismo sigue estándares internacionales de Protección de Datos Personales.

Certinet no hace tratamiento de Datos Personales Sensibles, ni de menores.

Los mecanismos automatizados generan registros de actividades de los Titulares/Usuarios, tendientes a establecer patrones de actividad y tráfico al interior del sitio. Se trata de información sobre la URL y nombre de dominio desde la cual se accede al sitio web, el número IP y browser que utiliza el Titulare/Usuario, el día y hora de acceso al sitio.

Certinet no utiliza cookies u otros mecanismos similares para recolectar información personal de los Titulares/Usuarios

Las peticiones formales de inscripción a los Titulares/Usuarios, recopilan básicamente su nombre, teléfono, casilla electrónica y domicilio. Cada vez que estos datos se soliciten y registren, se hará de manera voluntaria al usuario. Certinet recopila esta información para identificar al Titular/Usuario que establece una relación contractual con Certinet a través de su sitio web y con el sólo objeto de dar cumplimiento a los derechos y obligaciones del respectivo contrato.

Certinet se compromete a procesar los datos personales de manera legal, según Ley 19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma, sus Reglamentos y Guías de Acreditación, de manera justa y transparente.

- Solo se recopilarán datos personales para fines específicos y legítimos, y no se procesarán de manera incompatible con esos fines.
- Los datos personales serán adecuados, relevantes y limitados a lo necesario para los fines para los que se procesan.
- Se tomarán medidas para garantizar que los datos personales sean precisos y se mantengan actualizados.

- Se conservarán los datos personales durante el tiempo necesario para cumplir con los fines para los que se recopilaron según la normativa de la Ley 19.799.
- Se aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales.

4.2 Recopilación y Uso de Datos

- Certinet recolecta, mantiene, usa, publica y distribuye la información personal vinculada con los Titulares/Usuarios, en los términos indicados en su Política de Privacidad, publicada en www.certinet.cl, y verificando que los datos sean correctos, completos y adecuados para cumplir con los fines para los que serán utilizados.
- Certinet recopilará y utilizará datos personales solo para fines específicos, como la prestación de servicios, la gestión de recursos humanos, la comunicación con clientes, etc.
- En caso que sea necesario se obtendrá el consentimiento de las personas para el procesamiento de sus datos personales y se informará de manera clara sobre cómo se utilizarán los datos.

5. De la Información de los Certificados Digitales

a. El contenido de los Certificados emitidos por Certinet y el Registro Público de Certificados administrado por Certinet son una fuente de libre acceso público, y puede contener datos personales del Titular/Usuario que sean necesarios para dicho efecto.

b. La información proporcionada por el Titular/Usuario, será utilizada y tratada únicamente por Certinet para la emisión de certificados y la mantención del Registro Público de Certificados.

c. La información no será revelada ni comercializada a terceros, sin el consentimiento previo otorgado en forma electrónica, por el Titular/Usuario al Sitio de Certinet www.certinet.cl a través de enlaces de sitios de propiedad o administración de terceros, podrá facultar a estos últimos, a registrar la información solicitada en dichos sitios, sin responsabilidad alguna para Certinet.

d. Lo anterior no regirá si media alguna disposición legal, resolución judicial o administrativa que obligue a Certinet a someter materias sujetas a confidencialidad al conocimiento de tribunales de Justicia, instituciones o entidades facultadas por ley y que actúen dentro del ámbito de sus atribuciones.

e. Certinet se obliga a utilizar la información y datos obtenidos respetando íntegramente los términos de la N° 21.719 que Regula la Protección de Datos Personales y crea la Agencia de

Protección de Datos Personales y los derechos establecidos en la ley 19.496 sobre protección de los derechos del consumidor.

6. Roles y responsabilidades en la Aplicación de la Política

Certinet ha designado a un Oficial de Protección de Datos de la organización y es el responsable de supervisar el cumplimiento de esta política y de las leyes de protección de datos aplicables.

Todos los empleados y contratistas tienen la responsabilidad de cumplir con esta política y las directrices establecidas para la protección de datos.

6.1 Rol del Oficial de Protección de Datos (DPO)

El DPO es responsable de la privacidad en la empresa, que, con una función preventiva y proactiva, debe supervisar las políticas de privacidad y protección de datos para garantizar la puesta en marcha de esas políticas a través de todas las unidades en la empresa y se asegura de que la compañía procese los datos personales de manera efectiva de acuerdo con las leyes de protección de datos vigentes.

- **Supervisar el Cumplimiento de la Protección de Datos:** El DPO es responsable de garantizar que la organización cumpla con todas las leyes y regulaciones de protección de datos aplicables, como la Ley N° 21.719 que Regula la Protección de Datos Personales y crea la Agencia de Protección de Datos Personales y el Reglamento General de Protección de Datos (GDPR) en la Unión Europea u otras leyes nacionales de privacidad.
- **Asesorar a la Organización**: El DPO brinda asesoramiento experto a la organización y a su personal sobre cuestiones relacionadas con la protección de datos. Esto puede incluir la revisión de políticas y procedimientos, la realización de evaluaciones de impacto de protección de datos y la consulta sobre el cumplimiento normativo.
- **Gestionar Solicitudes de Derechos de los Interesados**: El DPO ayuda a gestionar las solicitudes de derechos de los interesados, como el derecho de acceso, rectificación, supresión, limitación del procesamiento, portabilidad de datos y oposición. Asegura que estas solicitudes se aborden de manera oportuna y de acuerdo con la ley.
- **Monitorear la Seguridad de los Datos:** El DPO supervisa la seguridad de los datos personales y trabaja para garantizar que los datos se procesen de manera segura. Esto puede incluir la evaluación de riesgos y la implementación de medidas de seguridad adecuadas.
- **Realizar Evaluaciones de Impacto de Protección de Datos (DPIAs):** Cuando sea necesario, el DPO participa en la realización de DPIAs para evaluar y minimizar los riesgos para la privacidad de los datos en proyectos o actividades específicas.
- **Actuar como Punto de Contacto con las Autoridades de Protección de Datos**: El DPO es el

punto de contacto principal entre la organización y las autoridades de protección de datos. Debe notificar a las autoridades de cualquier violación de datos y cooperar con ellas en investigaciones y auditorías.

- **Promover la Conciencia y la Formación en Protección de Datos:** El DPO ayuda a aumentar la conciencia sobre la protección de datos dentro de la organización, brindando formación y orientación a los empleados para garantizar que comprendan y cumplan las políticas y regulaciones de privacidad.
- **Actualizar Políticas y Procedimientos:** El DPO revisa y actualiza regularmente las políticas y procedimientos de protección de datos de la organización para asegurarse de que estén en línea con las últimas regulaciones y mejores prácticas.
- **Mantener Registros de Actividades de Tratamiento**: El DPO ayuda a mantener registros de todas las actividades de procesamiento de datos personales que realiza la organización, como parte de requisito legal.
- **Evaluar y Gestionar Riesgos:** El DPO evalúa los riesgos asociados con el procesamiento de datos personales y trabaja con la organización para implementar medidas para mitigar estos riesgos.

6.2 Rol de los Responsables del Tratamiento de Datos

La Nueva Ley N° 21.719 que Regula la Protección de Datos Personales y crea la Agencia de Protección de Datos Personales, impone importantes y estrictas obligaciones a los responsables y mandatarios de adoptar medidas de seguridad apropiadas al tratamiento específico.

La elección de estas medidas debe tomar en cuenta la naturaleza de los datos, el estado actual de la técnica y los costos de aplicación; la naturaleza, alcance, contexto y fines del tratamiento, la probabilidad de ocurrencia de riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados.

Las medidas de seguridad deben ser no solo técnicas, sino también organizativas, que permitan garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas para evitar la alteración, destrucción, pérdida, tratamiento o accesos no autorizados.

Los obligados directos a implementar medidas de seguridad son tanto responsables como encargados.

La falta de adopción de medidas de seguridad puede considerarse una circunstancia agravante de la responsabilidad en caso de infracciones (bajo la hipótesis de “haber puesto en riesgo la seguridad de los derechos y libertades de los titulares en relación a sus datos personales”) lo que se tomará en cuenta al determinar el monto de las multas.

Se debe tener en cuenta las siguientes consideraciones:

- La prueba es del responsable. La carga de la prueba de la existencia y el funcionamiento de las medidas de seguridad será siempre del responsable.
- La Ley N° 21.719 sugiere medidas de seguridad, como la seudonimización y el cifrado de datos; la capacidad de garantizar la confidencialidad, disponibilidad, integridad y resiliencia de los sistemas y servicios de tratamiento; restaurar la disponibilidad y el acceso a los datos en casos de incidentes de seguridad; llevar a cabo procesos de verificación, evaluación y valoración de las medidas, entre otras.
- Coordinación desde el origen con equipos de TI y de seguridad de la información. En estas obligaciones se requiere identificar las sinergias entre los equipos de compliance o los equipos técnicos; pues el trabajo de una sola de las áreas no será suficiente para acreditar una diligencia integral.
- Revisión de Políticas de Seguridad de la Información. Será necesario revisar y actualizar las políticas de seguridad de la información y sus procedimientos o protocolos asociados, para hacerlas coherentes con el cumplimiento de las nuevas obligaciones.

6.2.1 Cesión o Transferencia de Datos Personales (de Responsable a Responsable)

- Para transferir o ceder datos personales, el responsable debe contar con el consentimiento del titular, o estar frente a una cesión necesaria para el cumplimiento de un contrato o para la satisfacción de un interés legítimo del cedente o del cesionario.
- La cesión debe constar en un acuerdo escrito (Data Transfer Agreement) en el que se individualice a las partes, los datos que son objeto de la cesión, las finalidades del tratamiento y las demás estipulaciones que acuerden el cedente y el cesionario.

6.3 Rol de el o los encargados de Tratamiento de Datos

El lícito tratar datos personales a través de un tercero encargado o mandatario, usualmente, prestadores de servicios del responsable. Este deberá ceñirse a las instrucciones del responsable y al objeto del encargo que se regule entre ambos. Si el mandatario actúa en contravención de lo instruido por el responsable, se considerará como responsable directo para todos los efectos legales.

Para la comunicación responsable y encargado o mandatario, estos deberán celebrar un acuerdo de procesamiento de datos (Data Processing Agreement) en el que al menos consignen: el objeto del encargo, su duración, la finalidad del tratamiento, el tipo de datos personales tratados, las categorías de titulares, y los derechos y obligaciones de las partes.

El encargado no podrá delegar su mandato a terceros (sub-encargados) salvo que cuente con una autorización específica y por escrito del responsable.

Se debe tener en cuenta las siguientes consideraciones:

- Identificación de las operaciones de cesión y comunicación de datos. Deberán identificarse todas las operaciones en que el responsable transfiere y comunica datos y junto al contenido mínimo que deberá integrarse a los acuerdos de cesión y procesamiento.
- Gestión de proveedores. Certinet clasificará sus proveedores críticos y no críticos en relación con la intensidad y criticidad de su tratamiento de datos, e insertar en su relación las cláusulas, anexos o contratos independientes necesarios para regular el tratamiento de datos. Se establecerá las condiciones mínimas dictadas por el responsable, que deberá cumplir el encargado, particularmente las restricciones de uso de los datos, las medidas de seguridad, y las obligaciones de eliminación de los datos una vez termine la relación contractual que motiva el encargo.
- Cuestionario a Proveedores. Los responsables de tratamiento de datos someterán a sus proveedores a un cuestionario que les permita evaluar el grado de adhesión al cumplimiento de la Ley N° 21.719.

6.4 La Autoridad de Protección de Datos

Se crea la Agencia de Protección de Datos Personales para velar por la efectiva protección de los derechos que garantizan la vida privada y los datos personales junto con la fiscalización del cumplimiento de la ley.

La Agencia tendrá entre sus potestades el dictar instrucciones y normas generales obligatorias para regular las operaciones de tratamiento de datos personales; aplicar e interpretar administrativamente las disposiciones legales y reglamentarias, así como también las normas e instrucciones generales que dicte; fiscalizar el cumplimiento de la Nueva Ley; determinar infracciones e incumplimientos en que incurran los responsables; y desarrollar programas para difundir, promover e informar a la ciudadanía en relación con el respeto por la protección de datos entre otras funciones.

Certinet se adaptará a una nueva realidad que exige el relacionamiento con la autoridad, lo que era prácticamente inexistente o bien de carácter disperso y específico. También, la creación de la Agencia se relaciona la creación de un sistema de procedimientos administrativos y judiciales inéditos en Chile.

La Nueva Ley N° 21.719 que Regula la Protección de Datos Personales y crea la Agencia de Protección de Datos Personales, impone importantes y estrictas obligaciones a los responsables y mandatarios de adoptar medidas de seguridad apropiadas al tratamiento específico.

La elección de estas medidas debe tomar en cuenta la naturaleza de los datos, el estado actual de la técnica y los costos de aplicación; la naturaleza, alcance, contexto y fines del tratamiento, la probabilidad de ocurrencia de riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados.

Las medidas de seguridad deben ser no solo técnicas, sino también organizativas, que permitan garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas para evitar la alteración, destrucción, pérdida, tratamiento o accesos no autorizados.

Los obligados directos a implementar medidas de seguridad son tanto responsables como encargados.

La falta de adopción de medidas de seguridad puede considerarse una circunstancia agravante de la responsabilidad en caso de infracciones (bajo la hipótesis de “haber puesto en riesgo la seguridad de los derechos y libertades de los titulares en relación a sus datos personales”) lo que se tomará en cuenta al determinar el monto de las multas.

Se debe tener en cuenta las siguientes consideraciones:

- La prueba es del responsable. La carga de la prueba de la existencia y el funcionamiento de las medidas de seguridad será siempre del responsable.
- La Ley N° 21.719 sugiere medidas de seguridad, como la seudonimización y el cifrado de datos; la capacidad de garantizar la confidencialidad, disponibilidad, integridad y resiliencia de los sistemas y servicios de tratamiento; restaurar la disponibilidad y el acceso a los datos en casos de incidentes de seguridad; llevar a cabo procesos de verificación, evaluación y valoración de las medidas, entre otras.
- Coordinación desde el origen con equipos de TI y de seguridad de la información. En estas obligaciones se requiere identificar las sinergias entre los equipos de compliance o los equipos técnicos; pues el trabajo de una sola de las áreas no será suficiente para acreditar una diligencia integral.
- Revisión de Políticas de Seguridad de la Información. Será necesario revisar y actualizar las políticas de seguridad de la información y sus procedimientos o protocolos asociados, para hacerlas coherentes con el cumplimiento de las nuevas obligaciones.

6.5 Obligación de Reportar Brechas de Seguridad

La Ley N° 21.719 impone un deber concreto de informar a la Agencia –y también directamente a los titulares cuando se afecten datos sensibles, de menores de 14 años o relativos a obligaciones de carácter económico, financiero, bancario o comercial– por los medios más expeditos posibles y sin dilaciones indebidas, de las vulneraciones a las medidas de seguridad que impliquen un riesgo razonable para los derechos y libertades de los titulares y que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que se traten o la comunicación o acceso no autorizados a dichos datos.

Al respecto, la Política de Seguridad de Certinet considera el capítulo respecto Incidentes de Seguridad y su Reporte de acuerdo a los SLA definidos en los reglamentos de la Ley a las Agencias de Seguridad contempladas en la legislación y sus reglamentos.

Para tener un orden de magnitud de las multas, el incumplimiento de esta obligación configura una infracción grave cuya sanción es de multa de hasta 10.000 UTM y, en caso, de que el incumplimiento sea deliberado, se puede configurar una infracción gravísima con una multa de hasta 20.000 UTM

Para implementar el reporte oportuno de incidentes de vulneración de datos personales, se establecerá un Plan de respuesta a incidentes. Se implementará o actualizará los procedimientos y planes de respuesta a incidentes de seguridad, coordinando a priori las etapas de comunicación interna y externa, los equipos involucrados y sus responsabilidades. Esto permitirá minimizar el impacto de una brecha, y facilitará el cumplimiento de las obligaciones de notificación.

Documentación. La Ley N° 21.719 requiere registrar las comunicaciones, describir la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

6.6 Privacidad desde el Diseño y por Defecto y Evaluaciones de Impacto de Privacidad

La Ley N° 21.719 consagra un deber general de protección desde el diseño y por defecto, instaurando una norma que exigirá a los responsables la adopción de una perspectiva transversal, proactiva y preventiva en materia de protección de datos personales.

Se debe tener en cuenta las siguientes consideraciones:

- Adopción de medidas técnicas y organizativas desde el diseño de todas las iniciativas que involucren tratamiento de datos. La privacidad se transforma en un factor determinante en de cualquier modelo de negocios. Los responsables quedan obligados a adoptar medidas específicas que resguarden transversal y proactivamente la privacidad de los titulares,

durante todas las etapas que involucre la actividad, negocio o proyecto correspondiente. Para determinar las medidas se atenderá a:

(i) estado de la técnica;

(ii) costos de implementación;

(iii) naturaleza, ámbito, contexto y fines del tratamiento de datos; y

(iv) riesgos asociados.

- Elaboración de una Política de Privacidad desde el Diseño y por Defecto, que permita trazar internamente las directrices que definirán el actuar de la empresa en materia de privacidad, abarcando el antes, durante y después de cualquier actividad, negocio o proyecto que involucre tratamiento de datos personales. Esta política establece directrices de actuación, identifica fases de control, establece niveles de actuación según la criticidad de los riesgos, define la aplicación de evaluaciones de impacto de privacidad, y fijar criterios para implementar medidas de mitigación, entre otras materias.

6.7 Evaluaciones de Impacto de Privacidad (“PIA”).

La Ley N° 21.719 exige que, cuando una actividad de tratamiento de datos por su naturaleza, alcance, contexto, tecnología utilizada o fines, involucre un alto riesgo para los derechos de los titulares, se realice en forma previa una evaluación de impacto en protección de datos personales.

6.8 La Agencia publicará una lista orientativa de los tipos de tratamiento que requerirán PIA.

La infracción a esta obligación es altísima pues es sancionada como infracción gravísima, con una multa asociada de hasta UTM 20.000.

Se debe tener en cuenta las siguientes consideraciones:

- Deberán crearse los procesos que permitan elaborar un PIA, cumplidos que sean ciertos criterio de alto riesgo que se deberán establecer en la Política de Privacidad desde el Diseño y por Defecto.
- La Nueva Ley establece que estas evaluaciones deberán realizarse, entre otras, en los siguientes casos:

i En proyecto de evaluaciones sistemáticas de aspectos personales de los titulares basados en tratamientos automatizados, como la elaboración de perfiles.

ii En los escenarios de tratamiento masivo de datos o a gran escala.

iii Iniciativas que involucren el monitoreo o supervisión de los titulares en zonas de acceso público.

6.9 Transferencia Internacional de Datos

La Ley N° 21.719 regula la transferencia internacional de datos personales, estableciendo un listado cerrado de hipótesis en que se permite y otorgando a la Agencia amplias facultades para fiscalizar las operaciones, formular recomendaciones, adoptar medidas conservativas y en casos calificados, suspender temporalmente el envío de los datos.

Las operaciones de transferencia internacional de datos solo están autorizadas en los escenarios de:

- Cuando la transferencia se realiza a un país que proporcione niveles adecuados de protección. La Agencia determinará cuales son esos países, en una "decisión de adecuación".

- Quede amparada por cláusulas contractuales o normas corporativas vinculantes, y se establezcan garantías adecuadas -i.e., que contengan similares o mayores principios, derechos y garantías a aquellas que ofrece la Ley N° 21.719, y en particular, que otorguen derechos exigibles y acciones legales efectivas a los titulares de los datos.

- Quede amparada un modelo de cumplimiento o mecanismo de certificación con garantías adecuadas adoptados entre el responsable y el tercero receptor de datos.

En ausencia de estos elementos, se podrán realizar transferencias específicas y no habituales sólo cuando (entre otras):

- Exista consentimiento expreso para una transferencia internacional específica y determinada.
- Haya autorización expresa de la ley y para una finalidad determinada.

7. Nuevas Bases de Licitud para Tratar Datos Personales

Uno de los cambios en la Ley N° 21.719 es la consagración de nuevas "bases de licitud" o habilitantes legales que permiten el tratamiento de datos personales:

7.1 Consentimiento libre

Específico e informado del titular, que deberá manifestarse de forma previa e inequívocamente mediante una declaración verbal, escrita o por un medio electrónico equivalente o mediante un acto afirmativo del titular.

7.2 Ejecución o cumplimiento de una obligación legal

Ejecución o cumplimiento de una obligación legal cuando exista directamente una autorización legal para el tratamiento;

7.3 Datos relativos a obligaciones de carácter económico, financiero, bancario o comercial

Tratamiento de datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, incluyendo los datos referidos a la situación socioeconómica del titular, siempre que se haga en conformidad con lo dispuesto en el Titulo III de la Ley N° 21.719;

7.4 Celebración o ejecución de un contrato

Tratamiento de datos necesario para la **celebración o ejecución de un contrato** entre el responsable y el titular, incluyendo medidas precontractuales;

7.5 Intereses legítimos

Tratamiento de datos necesario para la satisfacción de **intereses legítimos** que no afecten los derechos y libertades del titular; y

7.6 Formulación, ejercicio o defensa

Tratamiento de datos necesario para la **formulación, ejercicio o defensa de un derecho** ante los tribunales de justicia u órganos públicos.

Esto requiere la Clasificación de datos y asignación de bases de legalidad. En términos prácticos, los responsables deberán identificar sus tratamientos de datos, para luego asociarlos a la base de legalidad correspondiente, que justifica el uso del dato para una determinada finalidad.

La clasificación de las actividades de tratamiento, los propósitos de uso y las distintas categorías de datos personales que el responsable trata, asociada a las bases de licitud que correspondan, es una operación que requiere se cuente con inventarios o catálogos de datos actualizados.

8. Principios de la Protección de Datos

La Nueva Ley recoge, en forma expresa y detallada, un listado de principios que regulan el tratamiento de los datos personales, que buscan orientar a responsables y encargados en cómo cumplir las obligaciones, y guiar la interpretación de las autoridades en su supervisión y fiscalización.

8.1 Principio de Licitud y Lealtad

Los datos personales sólo pueden tratarse de manera lícita y leal.

El responsable de datos debe poder demostrar que cuenta con una base de licitud que justifica el tratamiento que realiza. Por ello, será indispensable que los responsables de datos identifiquen las

fuentes de recolección de los datos personales, los propósitos de los tratamientos, y las bases de licitud asociadas a cada tratamiento. Una herramienta útil para este propósito será la elaboración de un Registro de Actividades de Tratamiento ("RAT").

8.2 Principio de Finalidad

Los datos personales sólo se pueden recolectar con fines específicos, explícitos y lícitos.

No se podrán tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que se trate de algún fin claramente compatible. Los fines del tratamiento deben informarse claramente al titular y deben ser específicos, sin declaraciones genéricas o abiertas en los avisos de privacidad.

Para ello, la organización debe ser capaz de identificar o etiquetar sus datos en relación con los propósitos autorizados para ellos, e implementar medidas para evitar que los datos se usen para fines diferentes.

8.3 Principio de Proporcionalidad

Los datos personales deben limitarse estrictamente a los necesarios, adecuados y pertinentes a los fines del tratamiento, y no deben conservarse por más tiempo que el necesario cumplir con esos fines.

Bajo la Ley N° 21.719 se considera una infracción grave (multa de hasta 10.000 UTM) efectuar tratamientos innecesarios en relación con los fines correspondientes, por lo que los responsables deberán asegurarse que los datos utilizados en cada operación sean siempre los estrictamente necesarios, adecuados y pertinentes en relación con los fines respectivos. Para ello, será altamente recomendable que Certinet implemente procesos que favorezcan la minimización de datos, preparar e implementar políticas de control de acceso para evitar el acceso y comunicaciones excesivas o innecesarias de datos personales durante la ejecución de procesos internos de la empresa.

8.4 Principio de Responsabilidad

Quien realiza el tratamiento es legalmente responsable del cumplimiento y debe acreditarlo

La carga de la prueba del cumplimiento de las obligaciones recaerá siempre en el responsable, quien debe no solo cumplir, sino estar preparado para demostrar que cumple. En el principio de legalidad: El responsable deberá ser capaz de acreditar la licitud del tratamiento de datos personales que realiza.

En las bases de licitud: El responsable deberá acreditar la licitud del tratamiento de datos.

En obligaciones de seguridad: el responsable debe acreditar la existencia y el funcionamiento de las medidas de seguridad.

En transferencia internacional: Corresponderá al responsable de datos que efectuó la transferencia internacional de datos, acreditar que ésta se practicó de conformidad a las reglas.

8.5 Principio de Transparencia: El aviso de Privacidad

El responsable debe entregar al titular toda la información necesaria para el ejercicio de sus derechos y que les permita entender en detalle las prácticas del tratamiento de sus datos.

La entrega y facilitación de esta información se traduce en la redacción y disponibilización de sus políticas de tratamiento de datos, la principal de ellas (pero no la única) el aviso de privacidad. La redacción debe ser clara e inequívoca y la accesibilidad debe ser permanente y gratuita. Así, por ejemplo: Las políticas de privacidad de clientes deben estar disponibles en los sitios web de un e-commerce.

Las políticas de privacidad de trabajadores deben estar disponibles en la intranet de la organización. Las políticas de aplicación corporativa deben ser conocidas, accesibles y sencillas

Contenido mínimo de las políticas de privacidad. La Nueva Ley la Ley **N° 21.719** establece un contenido mínimo – bastante extenso – de la información a entregar al titular en la política de privacidad. Esto incluye, entre otros: la individualización del responsable y sus datos de contacto, su representante legal y la identificación del encargado de prevención, si existiere; la identificación del medio tecnológico mediante el cual los titulares puedan realizar sus solicitudes; las medidas de seguridad; el periodo durante el que se conservarán los datos personales; la existencia de decisiones automatizadas, incluida la elaboración de perfiles.

8.6 Principio de Confidencialidad

El responsable y quienes tengan acceso a los datos deben guardar secreto de estos incluso aun después de finalizar la relación con el titular.

Los responsables deben establecer controles para que sus dependientes o proveedores que accedan a los datos, cumplan el deber de secreto o confidencialidad. Lo anterior implica, por ejemplo, adecuar las cláusulas de confidencialidad (NDA) con trabajadores y proveedores que traten datos personales en calidad de mandatarios.

El principio de confidencialidad se encuentra íntimamente relacionado con los deberes de seguridad, y su no observancia se sanciona como infracción grave (multa de hasta 10.000 UTM)

9. Compromiso de Resguardo de información y Protección de Datos Personales de Titulares/Usuarios

Compromiso de Resguardo de información y Disposiciones legales que regulan la protección y no divulgación de ésta.

Los resguardos contractuales que se les facilita a los Titulares/Usuarios se encuentran en los documentos, Contrato de Suscripción de Firma Electrónica Avanzada firmado por la persona que obtiene un Certificado Digital. Las disposiciones mencionadas se enlistan a continuación.

9.1 Resguardo Información.

El Titular/Usuario garantiza a Certinet y a cualquier tercero que confíe en su Certificado que;

a. toda la información que suministró a Certinet en la Solicitud de Certificado es veraz y actualizada.

b. ninguna información suministrada, incluyendo la dirección de correo electrónico, infringe los derechos de terceros, por ejemplo, la propiedad intelectual.

c. la información suministrada en la Solicitud de Certificado, incluyendo la dirección de correo electrónico, no ha sido ni será utilizada para cualquier propósito ilegítimo o contrario a la ley;

d. el "Titular/Usuario" autoriza a Certinet que obtenga datos de identificación personales que le permitan corroborar los datos e identidad del "Titular/Usuario" para efecto de enrolamiento y generación de su certificado firma electrónica de modo de autentificar fehacientemente la identidad del "Titular/Usuario". Esto de acuerdo con la ley chilena 19.799 de Firma Electrónica y las leyes internacionales de privacidad, protección y resguardo de datos personales, Certinet utiliza dichos datos sólo con el propósito de registrar al "Titular/Usuario" y resguardar las evidencias de acuerdo a normas y estándares internacionalmente reconocidos.

e. Certinet reconoce y adhiere a la política de privacidad de Google Play de Apple Store y al servicio Clave Única del Registro Civil.

f. el "Titular/Usuario" es la única persona que ha tenido desde el momento de su generación y seguirá teniendo en el futuro posesión de su clave privada y ningún tercero no autorizado ha tenido o tendrá accesos a dicha clave privada;

g. el "Titular/Usuario" es la única persona que ha tenido desde el momento de su generación y seguirá teniendo en el futuro posesión de cualquier frase de comprobación, Número de identificación personal (PIN), software o mecanismo de hardware que protege su clave privada y ningún tercero no autorizado ha tenido o tendrá acceso a dichos elementos;

h. el “Titular/Usuario” utilizará su Certificado exclusivamente para propósitos autorizados y legales, de conformidad con el presente Acuerdo de Titular/Usuario;

i. el “Titular/Usuario” utilizará su Certificado en carácter de Titular/Usuario final y no como una Autoridad Certificadora;

j. cada firma electrónica y/o Electrónica Avanzada creada utilizando la clave privada que se corresponde con la clave pública contenida en el Certificado es la firma del “Titular/Usuario” .

k. Certificado ha sido aceptado y está vigente (es decir no ha vencido ni ha sido revocado) en el momento en que dicha firma electrónica es creada; y

l. el “Titular/Usuario” ha prestado su total conformidad con el presente Acuerdo de Titular/Usuario como condición esencial para la obtención de un Certificado.

El incumplimiento de cualquiera de estos literales será de su exclusiva responsabilidad civil, penal y/o administrativa

9.2 Directrices para los Colaboradores

Todos los colaboradores, personal a honorarios y terceros deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones, según lo establecido en la presente y la ley la Ley N° 21.719 y los documentos relacionados.

Sin perjuicio de lo anterior, los colaboradores, personal a honorarios y terceros, que trabajan en el tratamiento de los datos personales o sensibles estarán obligados a guardar secreto sobre el mismo, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como, asimismo, sobre los demás actos y antecedentes relacionados con la Ley N° 21.719.

Por lo tanto, los datos personales o sensibles, indistintamente del medio en que estén contenidos, deberán ser protegidos y resguardados adecuadamente por quienes tienen el deber de manipularlos, garantizando razonablemente su privacidad a través de la implementación de procedimientos y controles para su tratamiento.

Mediante los respectivos contratos de trabajo o de servicios, los colaboradores, personal a honorarios y terceros se comprometerán a utilizar la información solamente para la finalidad legítima específica en que se basó que pudieran acceder a la información y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, sea natural o

jurídica, salvo autorización previa y escrita del Responsable del Activo de que se trate conforme a las normas a que se hace referencia en la presente política

9.3 Directrices de Sistemas y Aplicaciones

Todo sistema o aplicación en que se traten datos personales deberá ser diseñado y desarrollado de manera tal que se dé cumplimiento a las obligaciones de reserva o secreto, de acuerdo con la naturaleza de la información. De esta manera, los sistemas que tengan por objeto el tratamiento de datos sensibles deberán cumplir las reglas siguientes:

- **Privacidad por defecto**: Los sistemas y aplicaciones, por defecto, guardarán la privacidad de los datos, debiendo requerirse una acción consciente y trazable para cambiar el modelo de acceso a los datos. En este ámbito, los sistemas aplicaciones deberán incluir o encriptación de datos, de acuerdo con los requerimientos funcionales que se definan.

- **Seguridad en el diseño:** Los sistemas y aplicaciones deberán ser desarrollados de forma tal que incluyan sistemas de verificación permanente de brechas de seguridad. Asimismo, los sistemas deberán estar diseñados para adoptar las medidas urgentes y necesarias para el resguardo de los datos personales en caso de un incidente de seguridad que pudiere afectarlos

- **Segregación datos y de funciones:** El diseño de los sistemas deberá considerar perfiles diferenciados por competencias, de forma tal que sólo puedan acceder a los datos personales los profesionales que se encuentren legalmente facultados para acceder a ellos.

9.4 Difusión y Contacto

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- **Correo informativo.**
- **Entrega de una copia, como anexo en las nuevas contrataciones de la Empresa**

Para consultas relacionadas con esta Política de Protección de Datos, póngase en contacto con dpo@certinet.cl.

9.5 Cambios a la Política de Privacidad y Protección de Datos Personales

Certinet se reserva el derecho a modificar la presente Política de Privacidad y Protección de Datos, con el objeto de adaptarlas a cambios legislativos o doctrinales, a prácticas generales de la industria o a políticas comerciales de Certinet.

Las modificaciones a la Política de Privacidad y Protección de Datos serán debidamente anunciadas a los usuarios a través de esta misma página. Será responsabilidad del usuario mantenerse informado acerca de la Política de Privacidad vigente.

9.6 Derechos de los Interesados

- Certinet respetará los derechos de los interesados, incluyendo el derecho de acceso, rectificación, supresión y portabilidad de datos.
- Las solicitudes de ejercicio de derechos serán atendidas de manera oportuna y de acuerdo con la ley.
- Los usuarios podrán en todo momento acceder, rectificar cancelar u oponerse al tratamiento de sus datos personales que hayan sido registrados en el sitio web de Certinet directamente mediante las aplicaciones del sitio.
- Certinet confirmará al usuario el ejercicio de sus derechos de acceso, rectificación, cancelación u oposición en caso de ser procedentes mediante aviso enviado por correo electrónico.

9.7 Seguridad de Datos

- Certinet utiliza un sistema de encriptación SSL para proteger la transmisión de información que entregan los usuarios del sitio web de Certinet. Esta información es almacenada en forma segura, estableciendo mecanismos de control sobre las posibles pérdidas, mal uso, alteración o entrega no autorizada de dicha información.
- Se implementarán medidas de seguridad técnica y organizativa para proteger los datos personales contra el acceso no autorizado, la divulgación, la alteración o la destrucción.
- Se llevarán a cabo evaluaciones de riesgos y se realizarán auditorías de seguridad de datos periódicamente.

9.8 Transferencia de Datos

- Certinet asegurará que cualquier transferencia de datos personales ya sea en Chile o fuera de las fronteras cumpla con las leyes y regulaciones aplicables.
- Certinet no podrá compartir con terceros la información personal vinculada a los usuarios, salvo que exista consentimiento de quien entregó dicha información, expresado a través de medios físicos o electrónicos. No queda incluida por esta restricción:

- Aquella información que provenga de fuentes accesibles al público tales como las contenidas en guías telefónicas públicas, reportajes de prensa, publicaciones, zonas de chateo o boletines u otras similares; y
- Aquella información que sea requerida por la ley, por una orden judicial o administrativa con motivo de una investigación o requerimiento de una autoridad pública en el ámbito de su competencia.

9.9 Formación y Concienciación

- Certinet proporcionará formación adecuada en protección de datos para todos los empleados y contratistas que manejen datos personales.

9.10 Evaluación de Impacto de Protección de Datos (DPIA)

- Se llevarán a cabo evaluaciones de impacto de protección de datos cuando sea necesario para evaluar y mitigar riesgos para la privacidad de los datos.

9.11 Auditorías y Revisión

- La política de protección de datos se revisará regularmente y se actualizará según sea necesario para cumplir con las leyes y regulaciones cambiantes y las mejores prácticas.

10. Nuevo Catálogo de Derechos de los Titulares

Certinet reconoce los derechos de los titulares (antiguamente llamados derechos ARCO) que son la piedra angular de la Ley N° 21.719 que modifica este catálogo reconociendo nuevos derechos y robusteciendo otros.

10.1 Derecho de Acceso

Para saber si sus datos están siendo objeto de tratamiento, su origen, la finalidad del tratamiento, las categorías de destinatarios, el plazo de conservación y la lógica aplicada a la toma de decisiones automatizadas si aplicare.

Los responsables deben siempre entregar la información solicitada, salvo disposición legal en contrario.

10.2 Derecho de Rectificación

Para solicitar la modificación de datos inexactos, desactualizados o incompletos.

Rectificados que sean los datos, los responsables deberán comunicar la rectificación a los terceros a los que los hubiese comunicado o cedido, salvo cuando aquello represente un esfuerzo desproporcionado.

10.3 Derecho de Cancelación

Para solicitar la eliminación (“cancelación” o “supresión”) de los datos, bajo ciertas circunstancias.

El titular puede solicitar la eliminación de sus datos cuando éstos ya no sean necesarios para

los fines que fueron recopilados; cuando se revoque el consentimiento; cuando los datos sean obtenidos o tratados ilícitamente; cuando los datos estén caducos; cuando deban suprimirse para el cumplimiento de una sentencia u obligación legal y cuando se hubiese ejercido el derecho de oposición y no exista otra base de licitud para su tratamiento.

En Certinet, cuando el tratamiento sea necesario para el cumplimiento de una obligación legal o contractual no procederá este derecho.

10.4 Derecho de Oposición

Para oponerse a un tratamiento específico o determinado de sus datos, bajo ciertas circunstancias.

Puede un titular oponerse a un tratamiento específico de sus datos, cuando éste se fundamente en el interés legítimo del responsable de datos; cuando se realice solo con fines de marketing directo; o respecto de datos obtenidos de una fuente de acceso público, sin otra base de licitud.

10.5 Derecho de Oposición a Decisiones Individuales Automatizadas y Elaboración de **Perfiles**

Para no ser objeto de decisiones, basadas en el tratamiento automatizado de sus datos personales, cuando produzca efectos jurídicos en él o le afecten significativamente.

No existirá este derecho cuando

- La decisión sea necesaria para la celebración o ejecución de un contrato
- Exista consentimiento del titular
- Lo señale la ley

En Certinet, el responsable debe facilitar el derecho del titular a obtener una explicación, la intervención humana, a expresar su punto de vista y a solicitar la revisión de la decisión.

10.6 Derecho de Bloqueo

Para solicitar la suspensión temporal del tratamiento cuando se formule una solicitud de rectificación, supresión u oposición, y mientras ésta no se resuelva.

10.7 Derecho de Portabilidad

Para solicitar una copia de sus datos en un formato electrónico genérico e interoperable, y a comunicarlos o transferirlos a otro responsable.

10.8 Atención solicitudes de Titulares

Certinet preparará protocolos para la recepción de solicitudes de ejercicio de derechos ARCO, identificando a los stakeholders involucrados la recepción, calificación, procesamiento y respuesta de las solicitudes.

La información relativa a los titulares estará debidamente organizada y clasificada, para permitir responder oportunamente a las solicitudes.

Se establecerá medidas de autenticación para asegurarse que no ocurran brechas de seguridad por el ejercicio de derechos ARCO de parte de titulares fraudulentos.

La Ley N° 21.719 requiere que los responsables implementen “mecanismos y herramientas tecnológicas” que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz. En consecuencia, Certinet dispondrá en su plataforma www.certinet.cl la disponibilidad de las funciones donde el titular pueda ejercer sus derechos.

Los responsables de datos deberán acusar recibo y pronunciarse por escrito en a lo más 30 días corridos desde el ingreso de la solicitud, teniendo en consideración además que el titular podría solicitar el bloqueo temporal de sus datos.

---------- FIN del Documento ----------

Signed by:Roberto Eduardo Fernando Ri
Signed at:2025-08-06 14:54:00 -03:00
Reason:Apruebo este documento

Roberto Riveros CertiNet

Gerente General

Signed by:Ignacio Gonzalo Infante Pinto
Signed at:2025-08-06 12:54:57 -04:00
Reason:Apruebo este documento

Ignacio Infante Pinto CertiNet

Oficial de Seguridad