Política Global de Protección de datos Personales



Este documento contiene información propietaria de Indexa S.A, Global Electronic Connection Bussiness S.A y Asesorías y Gerenciamientos de Servicios Ltda., que ha sido preparada estrictamente con el propósito de ser utilizada en las operaciones de las Empresas y no podrá ser proporcionada, refraseada o revelada parcial o totalmente a terceros sin la autorización expresa del Comité de Seguridad de la Información.

ÍNDICE

CSMS1900.1. INTRODUCCIÓN 3
CSMS1900.1.1. Objetivo 3
CSMS1900.1.2. Alcance 3
CSMS1900.1.3. Roles y responsabilidad 3
CSMS1900.1.4. Comunicación 4
CSMS1900.1.5. Vigencia 4
CSMS1900.1.6. Definiciones 5
CSMS1900.2. TRATAMIENTO DE DATOS PERSONALES 6
CSMS1900.2.1. General 6
CSMS1900.2.2. Tratamiento de datos personales 7
CSMS1900.2.3. Medición 8
CSMS1900.2.4. Monitoreo y control 9
CSMS1900.2.5. Requerimiento de información 9
CSMS1900.3. POLÍTICAS 10
CSMS1900.4. REPORTE DE INCIDENTES O QUIEBRES 11
CSMS1900.5. ACCIONES DISCIPLINARIAS 12
CSMS1900.6. DOCUMENTOS Y REFERENCIAS 12

CSMS1900.1. INTRODUCCIÓN

CSMS1900.1.1. Objetivo

El propósito de este documento es formalizar el marco de trabajo que Indexa ha establecido para proteger, tratar y resguardar los datos personales. Por tanto, se han definido los criterios de control y los lineamientos de protección que garantizan el correcto manejo de esta información en el desarrollo de los procesos y ejecución de operaciones de la empresa. Con el objeto de:

- Garantizar el derecho constitucional del respeto y protección a la vida privada de las personas, así como la protección de sus datos personales, *(artículo 19 N°4 de la Constitución Política de la República[1]),* asegurando que el tratamiento de datos cumpla con la Ley sobre Protección de la Vida Privada.
- Informar a las personas los mecanismos por medio de los cuales Indexa trata sus datos personales en su calidad de responsable y/o encargado de datos, el período de conservación y destinatarios previstos a quienes podrá comunicar dichos datos personales.
- Poner en conocimiento de los titulares de datos personales los derechos que pueden ejercer respecto de ellos, los resguardos que Indexa, toma para garantizar su protección, así como toda otra información relevante al respecto.
- Fomentar la cultura de datos en la organización

CSMS1900.1.2. Alcance

La presente política es de aplicación general y abarca todos los aspectos relacionados con la administración, distribución, control, acceso, almacenamiento, tratamiento y destrucción de datos de carácter personal sean estos de colaboradores propios de la organización y/o datos que como proveedor(encargado) se deba tratar única y exclusivamente para los fines acordados contractualmente para la prestación del servicio contratado.

CSMS1900.1.3. Roles y responsabilidad

General

Son responsables de lo descrito en este documento: los comités corporativos *(continuidad, seguridad y riesgo)*, las gerencias, los administradores de la plataforma tecnológica y todos los funcionarios que utilicen, administren, traten, almacenen, y/o interactúen con datos personales.

Específicas

Gerencia de Desarrollo y tecnología: equipo multidisciplinario encargado de proporcionar todas las herramientas de almacenamiento, tratamiento, control, transmisión, destrucción y/o resguardo de datos personales, en formato digital.

Gerencia de Operaciones: equipo multidisciplinario encargado de proporcionar el almacenamiento, tratamiento, control, transporte y resguardo de datos personales registrados de forma física, de los clientes Indexa.

[1] Garantiza a todas las personas el derecho al respeto y protección de la vida privada y honra de la persona y su familia. Además, asegura la protección de los datos personales, constituyendo una base fundamental para la privacidad.

RRHH y finanzas: área encargada de recopilar, almacenar, custodiar, actualizar y destruir la información de carácter personal de los funcionarios de indexa conforme a las especificaciones del ordenamiento jurídico vigente, además de resguardar su confidencialidad, disponibilidad e integridad.

Comité de Gerencia: equipo multidisciplinario responsable de velar por el resguardo, tratamiento, almacenamiento, protección y destrucción de los datos personales *(físicos y lógicos)* en alcance a su gestión, conforme a las especificaciones legales que regula esta materia.

Comité de seguridad de la información: equipo multidisciplinario encargado de apoyar la gestión de datos de carácter personal conforme a la ley.

Contraloría: Responsable de evaluar de forma independiente el cumplimiento de la normativa de protección de datos personales, verificando la efectividad de los controles implementados, la adecuada gestión de riesgos, la correcta aplicación de los procedimientos y la integración del modelo con otros sistemas de control de la organización. Asimismo, deberá reportar sus conclusiones de auditoría a la alta dirección.

Delegado de protección de datos personales[2]: responsable de supervisar el cumplimiento de la normativa de protección de datos personales en la organización, asesorando a las distintas áreas en la correcta aplicación de la ley, evaluando los riesgos asociados al tratamiento de datos, coordinando la gestión de incidentes desde el punto de vista regulatorio y actuando como punto de contacto con la autoridad competente. Asimismo, deberá promover la implementación de buenas prácticas y la mejora continua del modelo de protección de datos.

El Designado de Protección de Datos Personales actuará con independencia en el ejercicio de sus funciones y será el punto de contacto con la autoridad reguladora en materia de protección de datos personales, velando por el cumplimiento de la normativa vigente y la correcta implementación de controles

CSMS1900.1.4. Comunicación

El comité de seguridad de la información debe asegurar que todos los funcionarios que interactúen con datos personales estén debidamente familiarizados con esta política. Para esto, se efectuarán actividades de difusión y capacitación que mantengan informada a la organización respecto a la protección de datos, su manejo y administración.

CSMS1900.1.5. Vigencia

Esta política se encuentra vigente a partir de 01-09-2020, El Comité de Seguridad de la información quien es el propietario de este documento debe revisar y actualizar el mismo, al menos una vez al año o por directrices entregadas por la alta dirección o como consecuencia de

- Nuevas normas legales o reglamentarias o nuevos instrumentos internacionales.
- Actualización normativa vigente
- Cambios en los procesos, tecnologías o actividades de tratamiento
- Resultados de auditorías internas o externas
- Recomendaciones o instrucciones de la Agencia u otras autoridades fiscalizadoras.
- No conformidad de la alta dirección y/o de órganos reguladores

[2] **Nota:** esta tarea es realizada por el gerente de desarrollo y tecnología dado que en el alcance de sus funciones participa en la evaluaciones de riesgo, diseño de productos y servicios, aplicación de controles interno, la detección de vulnerabilidades y en el monitoreo y cumplimiento de los cambios regulatorios.

Sin perjuicio de lo anterior, la Política deberá ser revisada, de manera inmediata, y modificada en su caso, cuando:

- Se detecten incumplimientos o brechas de seguridad relevantes por vicios contractuales, incumplimiento a disposiciones administrativas o tratamiento de datos no conforme a la ley.
- Se produzcan cambios organizacionales de carácter estructural.
- Se comiencen a realizar actividades de tratamientos de datos personales de alto riesgo.
- Ineficiencia en la implementación, mantención, control, administración y ejecución de la gestión de seguridad utilizada para preservar la confidencialidad, disponibilidad e integridad de los datos de carácter personal.

CSMS1900.1.6. Definiciones

Se entiende por:

Almacenamiento de datos
Conservación o custodia de datos en forma digital o física.

Bloqueo de datos
Suspensión temporal de cualquier operación de tratamiento de los datos almacenados.

Comunicación o transmisión de datos
Dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular.

Datos personales
Datos de carácter individual concernientes a personas naturales.

Datos personales sensibles
Datos referente a cualquier característica físicas o morales del individuo o hechos o circunstancias de su vida privada.

Eliminación de datos
Destrucción de datos almacenados en registros físicos o bancos de datos.

Fuentes accesibles al público
Registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

Modificación de datos
Cambio en el contenido de los datos almacenados en registros o bancos de datos.

Registro o banco de datos
Conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

Titular de datos
Persona natural a la que se refieren los datos.

Tratamiento de datos
El tratamiento de datos personales es cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales.

CSMS1900.2. TRATAMIENTO DE DATOS PERSONALES

CSMS1900.2.1. General

Indexa, debe generar los mecanismos de control que salvaguarden la información, de carácter personal, considerando todas las instancias que conforman su ciclo de vida a fin de preservar su confidencialidad, disponibilidad e integridad. Por otro lado, debe proporcionar los medios que permitan al titular de los datos a ejercer los derechos consagrados en la ley.

Detalle derechos

Derecho de acceso: facultad del titular de los datos a obtener información, respecto a sus datos personales, que permita conocer el propósito, origen, tipo y destinatarios de su tratamiento.

Derecho de rectificación: facultad del titular de datos para requerir la modificación o rectificación de aquella información de su titularidad, consignada de manera errónea, inexacta, incompleta o equívoca.

Derecho de supresión/cancelación: facultad del titular de la información para solicitar y obtener del responsable que suprima o elimine sus datos personales, cuando su tratamiento carezca de fundamento legal o en conformidad de las causales previstas en la ley.

Derecho de oposición: facultad del titular de la información para oponerse al tratamiento de sus datos personales o suspender dicha actividad conforme a la ley.

Derecho de portabilidad: facultad del titular de la información para solicitar y obtener del responsable del tratamiento una copia de sus datos personales en un formato electrónico, estructurado, genérico y de uso común, que permitan ser operados por distintos sistemas, a fin de poder comunicarlo y/o transferirlos a otros responsables de datos.

Las personas podrán hacer ejercicio de estos derechos por medio de “Procedimiento de gestión de requerimientos de datos personales”. Por medio de este procedimiento de contacto también podrán consultar por toda otra información adicional o complementaria relacionada con su ejercicio.

Sin perjuicio de lo anterior, la empresa está facultada a no modificar, cancelar, bloquear o eliminar datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, afecte el interés Nacional o su almacenamiento sea por mandato judicial, según lo dispuesto en el artículo 15 de la ley 19.628.[3]

Cuando el tratamiento de datos personales pueda implicar un alto riesgo para los derechos y libertades de los titulares, la organización deberá realizar evaluaciones de impacto en protección de datos personales (EIPD), conforme a la normativa vigente.

[3] El artículo 15 de la Ley 19.628 sobre Protección de la Vida Privada en Chile establece una excepción importante: no se puede solicitar la modificación, cancelación o bloqueo de datos personales cuando estos sean almacenados por **mandato legal**, fuera de los casos expresamente previstos en la ley.

CSMS1900.2.2. Tratamiento de datos personales

El tratamiento de datos personales sólo se lleva a cabo con la autorización expresa de la institución cliente y/o colaborador de la organización, quienes facultan a Indexa para: tratar, procesar, reprocesar y divulgar la información según los fines establecidos contractualmente entre las partes, no siendo estos datos tratados ulteriormente de manera incompatible con dichos fines.

Los datos tratados son adecuados, pertinentes y limitados a lo necesario en relación con los fines requeridos.

Sin perjuicio de lo anterior, Indexa deberá señalar el propósito del almacenamiento de los datos y la finalidad de los mismos, a su vez Indexa deberá proporcionar todas las medidas de resguardo que garanticen la privacidad de ellos.

Dentro de las responsabilidades adquiridas por la compañía, en virtud del tratamiento de los datos personales, se destacan los siguientes deberes:

- Conservar la información personal bajo las condiciones de seguridad idónea que impidan su adulteración, modificación, eliminación, consulta, uso o acceso no autorizado, el tiempo de almacenamiento será el necesario para los fines de tratamiento relacionados al servicio prestado.

- Actualizar, rectificar, bloquear y/o eliminar información personal acorde al ordenamiento jurídico y a las exigencias definidas en la ley y a requerimiento cliente.

- Permitir el acceso limitado y autorizado, a la información personal sólo a aquellos colaboradores que por perfil del cargo deban realizarlo.

- Tratar las consultas, reclamos y requerimientos de los titulares de la información en los términos señalados en la ley.

Datos personales proporcionados

Todo dato de carácter personal gestionado por Indexa, deberá ser autorizados por el dueño y/o responsable de este, como base de licitud. Encontrándose el detalle de estos y su tratamiento en catálogo de actividades (listado o registro que identifica la información), el que es actualizado constantemente según necesidad.

Detalle catálogo

- Categoría de datos que trata.
- Si trata dichas categorías de datos como responsable o encargado.
- El universo de titulares que comprenden sus bases de datos.
- La finalidad del tratamiento.
- La base de legitimidad del tratamiento.
- Los destinatarios previstos a los que se prevé comunicar los datos personales.
- Período de conservación de los datos personales.
- La fuente de la cual provienen los datos de las actividades de tratamiento de datos que realiza un responsable.

Almacenamiento de los datos y política de conservación y eliminación de datos personales

Indexa tratará sólo aquellos datos personales que resulten necesarios, adecuados y pertinentes para sus fines de tratamiento, los que conservará sólo por el período de tiempo necesario para cumplirlos.

Conservación y eliminación de datos personales

Indexa conservará los datos personales que trate por el tiempo indicado en el Catálogo al que se refiere la sección 2.2. de la presente política.

Una vez transcurrido el período de conservación, los datos se eliminarán física y lógicamente de los registros de Indexa de manera permanente.

Colaboración con otros organismos públicos

Cuando corresponda, Indexa podrá comunicar los datos personales que trata a organismos públicos, con los fines de:

- Comunicar a organismos del Estado sus datos personales, cuando esta comunicación sea estrictamente necesaria para el ejercicio de sus competencias y funciones legales, de acuerdo por el artículo 20 de la Ley N° 19.628.[4]
- Cuando sea necesario para otorgar beneficios al titular, evitar duplicidad de trámites para los ciudadanos o reiteración de requerimientos de información o documentos para los mismos titulares.
- Informar a entidades públicas o gubernamentales información estadística elaborada a partir de patrones de actividad, navegación, audiencia y caracterización general de los servicios.
- Comunicar a terceros información estadística elaborada a partir de los datos personales de sus usuarios, cuando de dichos datos no sea posible identificar individualmente a los titulares (datos disociados), de conformidad a la ley.

CSMS1900.2.3. Medición

El comité de seguridad de la información debe evaluar el cumplimiento de esta política, bajo los lineamientos de seguridad definidos en el marco normativo de Indexa S.A, a fin de asegurar la efectividad de los controles desarrollados por los propietarios y custodios de información, según los indicadores que ellos establezcan en cada uno de los procesos y/o servicios en alcance a su gestión. Asimismo, el comité es responsable de garantizar la efectividad de este documento y de evitar infracciones en materia de protección de datos.

[4] El artículo 20 de la Ley N° 19.628 sobre Protección de la Vida Privada en Chile establece que el tratamiento de datos personales por parte de organismos públicos debe limitarse a sus competencias legales, sin requerir el consentimiento del titular. Además, obliga a estas instituciones a informar sobre el propósito y manejo de los datos

CSMS1900.2.4. Monitoreo y control

De conformidad con la normativa vigente, Indexa S.A, adoptara todas las medidas necesarias para el resguardo de la seguridad de los datos personales y la privacidad de las personas, asegurando la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos; así como evitar su alteración, destrucción, pérdida, tratamiento o acceso no autorizado.

El espíritu de estas medidas se encuentra en la "Política de Seguridad de la Información" y "Politica de Ciberseguridad de la Organización" y marco normativo vigente de la empresa.

Independiente de lo anterior, cada gerencia dentro de su área de responsabilidad debera coordinar, controlar y monitorear las medidas de resguardo, definidas en el alcance de su función, para preservar la confidencialidad e integridad de los datos personales en el tratamiento y almacenamiento de los mismos.

El comité de seguridad de la información en conjunto con el delegado de protección de datos deben solicitar a los custodios y propietarios de información, según la frecuencia que estimen conveniente, detalles de los indicadores y controles utilizados en el resguardo y administración de los datos. Del resultado de esta gestión, se entregarán reportes a las unidades involucradas para que realicen las acciones correctivas, si amerita.

CSMS1900.2.5. Requerimiento de información

Todo requerimiento de información solicitado por el propietario de los datos o de la persona debidamente autorizada por él, será comunicado al cliente implicado para que este determine si se procede con la solicitud en conformidad a lo establecido en la ley 19.628 *(derechos ARCO).*

Sin perjuicio de lo anterior, es obligación de Indexa el asistir a sus clientes en la atención de derechos ARSOP (acceso, rectificación, supresión, oposición y portabilidad) y demás derechos aplicables, dentro de los plazos legales, realizando todas las acciones que le sean requeridas o que sean necesarias para tales fines.

CSMS1900.3. POLÍTICAS

Es política del grupo de empresas indexa establecer los siguientes principios, que deben ser respetados y seguidos por todos los funcionarios que participen o interactúen en el tratamiento y/o almacenamiento de datos personales.

Acceso
Toda información derivada de datos personales debe garantizar el acceso sólo a los titulares de la información o a las personas debidamente autorizadas por este último.

Durabilidad
La conservación de los datos personales no se extenderá más allá del plazo necesario para conseguir los fines que originaron su recolección o el tiempo señalado en la ley.

Finalidad
Todo dato personal debe ser empleado para los fines explícitos, lícitos y específicos que originaron su autorización. Si se utilizan para otros propósitos distintos a los informados al momento de su recepción, se debe solicitar autorización *(previa)* del titular de la información para este efecto.

Gratuidad
Todo acceso a los datos personales por parte de los titulares de la información será gratuito acorde a las leyes y el ordenamiento jurídico.

Inviolabilidad
Toda persona que administre, trate, almacene, controle o interactúe con datos personales conferidos a la empresa, debe garantizar su confidencialidad incluso, al terminar las relaciones laborales según las disposiciones legales que regulan esta materia.

Licitud
Todo dato personal almacenado y tratado por la empresa debe estar debidamente autorizado por el titular de la información y debe contar con su autorización expresa para este efecto.

Información
Toda incidencia, evento y/o problema de carácter personal debe ser informado a los entes interesados *(cliente, alta dirección y órganos reguladores)* según sus características, consecuencias e impactos.

Indexa comunicará, a los clientes afectados, las incidencias de datos personales considerando todo su ciclo de vida. Además de las medidas de contención utilizadas *(temporales o definitivas)* para superar la emergencia.

Toda comunicado enviado por indexa debe estar alineado a la exigencias regulatorias que norman el tratamiento de datos o leyes aplicables, según sus características técnicas.

Indexa informará la incidencias a los clientes implicados, lo antes posibles, según su prioridad de atención o plazos establecidos en la normativa vigente.

Legalidad
El tratamiento de los datos personales debe estar acorde de las exigencias del ordenamiento jurídico vigente y su tratamiento debe estar sujeto a sus disposiciones.

Indexa aplicará el principio de responsabilidad proactiva, debiendo no solo cumplir con la normativa de protección de datos personales, sino también ser capaz de demostrar dicho cumplimiento mediante la implementación de controles, registros, evaluaciones y mecanismos de supervisión continua.

indexa debe velar que los países receptores de información de carácter personal tengan un nivel de protección de datos adecuados en conformidad a la normativa nacional vigente. No obstante, si existen garantías contractuales aprobadas y consentimiento expreso del titular de la información se efectuará la transmisión de datos de forma segura.

Responsabilidad
Indexa y todo funcionario que administre, controle, manipule, almacene, trate y/o interactúe con datos personales o sensibles, son responsables de mantener la confidencialidad, integridad e inviolabilidad de la información tratada y almacenada bajo los lineamientos de esta política y la legislación vigente.

Seguridad
La información de carácter personal y sensible será manejada con todas las medidas técnicas, administrativas y humanas que garanticen la seguridad de los datos, a fin de disminuir y evitar cualquier tipo de adulteración, perdida, consulta, robo, uso y acceso no autorizado.

Veracidad
La información obtenida de datos personales y sujeta a tratamiento, debe ser exacta, actual y comprobable. En caso contrario, deberá ser suprimida o rectificada.

Prevención de uso indebido de información

El tratamiento de datos personales deberá realizarse evitando cualquier uso indebido de la información, acceso no autorizado o utilización con fines distintos a los establecidos, en conformidad con el Modelo de Prevención de Delitos de la organización y la normativa vigente.

CSMS1900.4. REPORTE DE INCIDENTES O QUIEBRES

Es responsabilidad de todos los funcionarios de indexa el informar cualquier sospecha o confirmación de quiebre a esta política u otra normativa de seguridad, a fin de minimizar el grado de exposición de la información y optimizar los tiempos de respuestas a la incidencia.

Si el funcionario identifica fallas y/o anormalidades en los controles, sistemas, servicios, herramientas o elementos utilizados en el desarrollo de sus funciones que pueda constituir un riesgo de seguridad, debe informar inmediatamente el hecho al comité de seguridad de la información *(por medio del email CSI@indexa.cl)*, para que establezca las pautas de trabajo y genere las acciones correctivas pertinentes y/o ejecutar procedimiento gestión de incidentes

En caso de incidentes que puedan comprometer obligaciones regulatorias, la organización deberá activar los procedimientos comunicacionales según alcance *(gestión de crisis o incidentes)* informando a: entes interesados, autoridades regulatorias en conformidad a los protocolos y normativas aplicables.

CSMS1900.5. ACCIONES DISCIPLINARIAS

Indexa podrá ejercer las acciones disciplinarias y legales cuando corresponda por el no cumplimiento con lo estipulado en esta política y/o en el manual de seguridad de la empresa.

Las acciones disciplinarias, dependencia de la gravedad de los hechos, consideran: amonestaciones, multas y el término inmediato del contrato de trabajo conforme a lo dispuesto en el reglamento interno de orden higiene y seguridad.

CSMS1900.6. DOCUMENTOS Y REFERENCIAS

- Norma chilena NCH-ISO27001.
- Norma chilena NCH-ISO27002.
- Ley 19.628
- Ley 21.719
- Modelo de Prevención de Delitos de la organización
- CNMC0000_PI_Política de continuidad de negocio.
- CSMS0000_PI_Política Global de seguridad de la información.
- ROGR001_PI_Política de Riesgo Operacional.
- CSMS0000_PI_Política de Gestión de Incidentes Tecnológicos.
- CSMS0700_PI_Política Global de Cifrados.
- CSMS0600_PI_Política global de ciberseguridad
- CSMS1000_N_Seguridad física y Medioambiental.
- CSMS1100_N_Norma de Seguridad física de la sala de servidores y equipamiento.
- CSMS3100_N_Respaldo de información.
- CSMS3000_N_Norma de clasificación y manejo de la información.
- CSMS0500_N_Administración de cuentas de usuario y claves de acceso.
- CSMS2500_N_Monitoreo y manejo de incidentes de seguridad.
- CSMS2600_N_Prevención de virus.
- CSPS2500_P_Procedimiento de Gestión de Incidentes.
- CSPS0500_P_Procedimiento de administración de cuentas de usuario y claves de acceso
- CSPS3100_P_Procedimiento de eliminación de información.
- CSPS3000_P_Procedimiento de clasificación de información

Historia de revisiones					
Cambio	**Descripción del cambio**	**Realizado por**	**Aprobado por**	**Identificación**	**Vigencia**
PRM19AG2020	Versión Inicial	MV	Comité de Gerencia	CSMS1900 V0.0	01Septiembre2020
VER28AB2021	Verificado con cambios	MV	CSI	CSMS1900 V0.1	04Mayo2021
VER06MY2022	Verificado sin cambios	MV	CSI	CSMS1900 V0.2	06Mayo2022
VER29MY2023	Verificado sin cambios	MV	CSI	CSMS1900 V0.3	29Mayo2023
VER16SE2024	Verificado Con cambios	MV	CSI	CSMS1900 V0.4	16Septiembre2024
VER25AG2025	Verificado Con cambios	SP	CSI	CSMS1900 V0.5	25Agosto2025
VER12FE2026	Verificado Con cambios	SP	CSI	CSMS1900 V 1.0	12Febrero2026