MANUAL DE PRIVACIDAD Y POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES

Fecha de Emisión: 01 de abril del 2025

Revisión: 2

Autor: Ab. Andrés Santiago Iturralde Terán

Revisó: Luis Alberto Iturralde Escobar

Aprobó: Cámara Universal de Accionistas

Fecha de Aprobación: 01 de abril del 2025

Contenido

1. INTRODUCCIÓN

El presente Manual de Privacidad y Políticas de Protección de Datos Personales (en adelante, el "Manual") tiene como objetivo establecer los lineamientos y principios que regirán el tratamiento de los datos personales en Consorcio LexCapital S.A.S. (en adelante, "la Empresa"). Este Manual será de obligatorio cumplimiento para todos los empleados, proveedores, clientes y terceros que tengan acceso a datos personales bajo custodia de la Empresa.

El Manual se ajusta a lo dispuesto en la Ley Orgánica de Protección de Datos Personales del Ecuador y otras normativas aplicables, garantizando el respeto a los derechos de los titulares de los datos personales. Además, este documento busca alinear las prácticas de la Empresa con los estándares internacionales de protección de datos, asegurando la transparencia, seguridad y confidencialidad en el manejo de la información personal.

2. OBJETIVO

- Objetivo General

El objetivo principal de este Manual es garantizar el cumplimiento de los derechos, principios y obligaciones establecidos en la Ley de Protección de Datos Personales, así como en las normativas secundarias y resoluciones emitidas por la Autoridad de Protección de Datos correspondiente. La Empresa se compromete a proteger la privacidad de los titulares de datos personales y a garantizar que el tratamiento de dichos datos se realice de manera segura, transparente y conforme a la ley.

- Objetivos Específicos

- Establecer los principios que guiarán a la Empresa en el manejo de los datos personales de sus clientes, empleados, proveedores y terceros.
- Crear mecanismos de control para garantizar la protección de los datos personales, incluyendo la implementación de medidas de seguridad técnicas, físicas y organizativas.
- Establecer lineamientos para la contratación de proveedores con enfoque en la protección de datos personales, asegurando que estos cumplan con las normativas aplicables.
- Implementar procesos de capacitación y concienciación para todos los empleados y colaboradores sobre la importancia de la protección de datos personales.
- Garantizar que los titulares de datos personales puedan ejercer sus derechos de acceso, rectificación, eliminación, oposición y portabilidad, entre otros.

3. RESPONSABILIDAD EN EL TRATAMIENTO DE DATOS

La Empresa es responsable de la custodia y conservación de los datos personales registrados. Sin embargo, la veracidad y autenticidad de los datos

proporcionados es responsabilidad exclusiva del titular de los datos. La Empresa se compromete a tratar los datos personales de manera confidencial y a implementar las medidas necesarias para prevenir el acceso no autorizado, la pérdida, alteración o divulgación de la información.

En caso de un mal tratamiento de los datos personales, los titulares afectados tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de las acciones legales pertinentes. La Empresa se compromete a investigar cualquier incidente relacionado con la protección de datos y a tomar las medidas correctivas necesarias para evitar futuras vulneraciones.

4. ÁMBITO DE APLICACIÓN

Este Manual es de aplicación obligatoria para todos los clientes, empleados, proveedores, accionistas, órganos directivos y terceros que tengan relación con la Empresa y que participen en el tratamiento de datos personales. Esto incluye, pero no se limita a:

- Empleados y colaboradores de la Empresa.
- Proveedores y contratistas que tengan acceso a datos personales.
- Clientes y usuarios de los servicios de la Empresa.
- Terceros que realicen actividades de tratamiento de datos en nombre de la Empresa.

El presente Manual aplica al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. También se aplicará cuando el tratamiento de datos personales se realice en cualquier parte del territorio nacional; o el responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional. Asimismo, se aplicará al tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios a dichos titulares o el control de su comportamiento en el Ecuador.

5. GLOSARIO DE TÉRMINOS

- Autoridad de Protección de Datos Personales: Autoridad pública independiente encargada de supervisar la aplicación de la LOPDP, su reglamento y resoluciones, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.

- Anonimización: La aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados.

- Autorización / Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento a tratar los mismos.

- Base de Datos o Fichero: Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.

- Dato Personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

- Dato Sensible: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

- Delegado de Protección de Datos (DPO): Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.

- Destinatario: Persona natural o jurídica que ha sido comunicada con datos personales.

- Elaboración de perfiles: Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o estándares relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.

- Encargado del Tratamiento de Datos Personales: Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.

- Fuente accesible al público: Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.
- Persona Identificable: Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente,

siempre y cuando esto no requiera plazos o actividades desproporcionadas.

- Responsable de Tratamiento de Datos Personales: Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o juntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

- Seudonimización: Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

- Titular: Persona natural cuyos datos son objeto de tratamiento.

- Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

- Tratamiento a gran escala: Es aquel que afecta a una gran cantidad de datos, referentes a un elevado número de titulares, procedentes de una amplia diversidad geográfica, y que pueden entrañar un riesgo a sus derechos y libertades. Para determinar cuándo se está en presencia de un tratamiento "a gran escala" se tendrán en cuenta: el número de interesados o titulares; el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento; la duración o permanencia de la actividad de tratamiento de datos; y el alcance geográfico de la actividad de tratamiento.

- Vulneración de la seguridad de los datos personales: Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

6. PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

- Juridicidad

Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la LOPDP, su Reglamento y la demás normativa y jurisprudencia aplicable.

- Lealtad

El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados. En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales.

- Transparencia

El tratamiento de datos personales deberá ser transparente por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro.

- Finalidad

Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular; no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en la LOPDP.

- Pertinencia y Minimización de Datos Personales:

Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.

- Proporcionalidad del tratamiento.

El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma de las categorías especiales de datos.

- Confidencialidad

El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en la LOPDP.

- Calidad y Exactitud:

Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad.

- Conservación:

Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento.

- Seguridad de Datos Personales:

Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales, frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto

- Responsabilidad Proactiva y Demostrada:

El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la LOPDP, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.

- Aplicación favorable al titular:

En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.

7. DERECHOS DE LOS TITULARES DE DATOS PERSONALES

Los titulares de datos personales tienen los siguientes derechos, reconocidos por la LOPDP:

- Derecho a la Información:

El titular tiene derecho a ser informado conforme los principios de lealtad y transparencia por cualquier medio sobre los fines del tratamiento, la base legal, tipos de tratamiento, tiempo de conservación, existencia de una base de datos, origen de los datos, otras finalidades, identidad y datos de contacto del responsable y delegado de protección de datos, transferencias o comunicaciones, consecuencias de la entrega o negativa de datos, efecto de

suministrar datos erróneos, posibilidad de revocar el consentimiento, existencia y forma de ejercicio de sus derechos, mecanismos de portabilidad y existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

- Acceso:

Derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el derecho a la información, sin necesidad de justificación alguna.

- Rectificación y Actualización:

Derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos.

- Eliminación

Derecho a que el responsable del tratamiento suprima sus datos personales cuando el tratamiento no cumpla con los principios de la ley, no sea necesario o pertinente para la finalidad, haya vencido el plazo de conservación, afecte derechos fundamentales, o el titular revoque el consentimiento.

- Oposición

Derecho a oponerse o negarse al tratamiento de sus datos personales cuando no se afecten derechos de terceros, la ley lo permita y no sea información pública, de interés público o por orden de ley; o el tratamiento tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles.

- Portabilidad

Derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables.

- Suspensión del Tratamiento

Derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos cuando el titular impugne la exactitud de los datos, el tratamiento sea ilícito y el interesado se oponga a la supresión, el responsable ya no necesite los datos, pero el interesado sí para reclamaciones, o el interesado se haya opuesto al tratamiento mientras se verifican los motivos legítimos.

- No ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas:

Derecho a no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en el o que atenten contra sus derechos y libertades fundamentales.

7.1. Ejercicio de Derechos:

Para efectivizar el ejercicio de los derechos establecidos en la LOPDP, la Empresa habilitará, preferentemente, herramientas o canales informáticos simplificados de fácil acceso para el titular, con la finalidad de receptar y atender oportunamente las solicitudes o peticiones formuladas que permitan y garanticen una interacción segura, fiable y rápida entre el responsable y el titular, sin perjuicio de que también puedan ser presentadas por medios físicos. Por lo tanto, se podrán habilitar plataformas digitales, centros de contacto, líneas telefónicas u otros mecanismos tecnológicos que se consideren idóneos para la presentación de las solicitudes por parte de los titulares. En todos los casos, el requirente deberá demostrar la titularidad o la representación legal para ejercer el derecho.

7.2. Contenido de la Solicitud

En la solicitud para el ejercicio de los derechos consagrados en la LOPDP, se hará constar:

- Los nombres y apellidos completos del titular, número de cédula de identidad o pasaporte y dirección domiciliaria o electrónica para notificaciones. Cuando se actúa en calidad de representante legal, se hará constar también los datos de la o del representado.

- De ser posible, la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados y cualquier otro elemento o documento que facilite la localización de los datos personales.

- Relación de lo que solicita expuesto de manera clara y precisa.

- Derecho o derechos que desea ejercer.

- A la solicitud se acompañará los documentos que acrediten la identidad o, en su caso, la representación legal o convencional del titular.

7.3. Requerimiento de Información Adicional

En caso de que la información constante en la solicitud requiera ser aclarada o ampliada, el responsable podrá requerir al titular, por una sola vez y dentro del término de cinco (5) días de recibida la solicitud, que la aclare o complete. El titular emplazado contará con el término de diez (10) días contados a partir del día siguiente en el que haya sido notificado, para aclarar o completar la solicitud. Si el titular aclara o completa la solicitud dentro del término concedido, el responsable le dará la debida atención, caso contrario, la archivará notificando este particular al titular con las razones de su decisión. El archivo del requerimiento inicial no impedirá la presentación de una nueva solicitud.

7.4. Registro de Solicitudes

La Empresa deberá registrar todas las solicitudes de ejercicio de derechos, incluyendo el detalle de la atención dada a las mismas. La Autoridad de Protección de Datos determinará el contenido de dichos registros.

7.5. Reclamo ante la Autoridad de Protección de Datos Personales

El titular de datos personales que encuentre motivos para creer que se han vulnerado sus derechos con la respuesta que el responsable ha dado a su solicitud, o que no haya recibido respuesta en el plazo establecido, podrá acudir a la Autoridad de Protección de Datos a presentar su reclamo, el cual se sustanciará conforme al procedimiento previsto en el Código Orgánico Administrativo y en la normativa complementaria que, para el efecto, emita la Autoridad de Protección de Datos.

8. TRATAMIENTO DE DATOS PERSONALES

- Recolección de Datos

La Empresa recolectará datos personales únicamente con la autorización expresa del titular, salvo en los casos previstos por la ley. La recolección de datos se realizará de manera transparente, informando al titular sobre la finalidad del tratamiento. Los datos personales podrán tratarse y comunicarse cuando se cuente con la manifestación de la voluntad del titular para hacerlo, la cual deberá ser libre, específica, informada e inequívoca.

- Uso de Datos

Los datos personales serán utilizados únicamente para las finalidades informadas al titular. La Empresa no utilizará los datos para fines incompatibles con los originalmente informados.

- Transferencia Internacional de Datos

En caso de transferencia internacional de datos, la Empresa garantizará que los datos sean protegidos de acuerdo con los estándares de la Ley Orgánica de Protección de Datos Personales. La Empresa solo transferirá datos a países que ofrezcan un nivel adecuado de protección o cuando se cuente con las garantías necesarias.

La transferencia o comunicación internacional de datos personales será posible si se sujeta a lo previsto en el Capítulo IX de la LOPDP o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales.

Por principio general, se podrán transferir o comunicar datos personales a países, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección, y que se ajusten a la obligación de cumplimiento y garantía de estándares reconocidos internacionalmente conforme a los criterios establecidos en el RLOPDP.

En caso de realizar una transferencia internacional de datos a un país, organización o territorio económico internacional que no haya sido calificado por la Autoridad de Protección de Datos como de tener un nivel adecuado de protección, se podrá realizar la referida transferencia internacional siempre que el responsable o encargado del tratamiento de datos personales ofrezca garantías adecuadas para el titular. Estas garantías incluyen el cumplimiento de principios, derechos y obligaciones en el tratamiento de datos personales en un estándar igual o mayor a la normativa ecuatoriana vigente, la efectiva tutela del derecho a la protección de datos personales a través de acciones administrativas o judiciales, y el derecho a solicitar la reparación integral, de ser el caso.

- Tratamiento de Datos de Niñas, Niños y Adolescentes.

Para el tratamiento de datos personales de menores de 15 años, se requerirá el consentimiento de su representante legal. Para el tratamiento de datos sensibles, así como para las decisiones basadas en valoraciones automatizadas de menores de edad, se requerirá el consentimiento expreso de su representante legal.

Los adolescentes a partir de los 15 años podrán otorgar su consentimiento explícito para el tratamiento de sus datos personales. Para este efecto, el responsable deberá proporcionar información clara, en un lenguaje sencillo propio de su edad, utilizando métodos que le permitan entender lo que ocurrirá con sus datos personales, las finalidades que se persiguen, los derechos que tiene y cómo ejercerlos y cualquier otra información necesaria para obtener su consentimiento explícito. También podrá otorgar el consentimiento del adolescente mayor de 15 años, quien ejerce la representación legal, sin perjuicio de que el adolescente, en cualquier momento, pueda revocar este consentimiento. El representante legal del adolescente no podrá revocar el consentimiento otorgado explícitamente por el adolescente en su calidad de titular.

El consentimiento obtenido para el tratamiento de datos personales de un menor de edad no podrá, bajo ninguna circunstancia, menoscabar el interés superior de la niña, niño o adolescente, conforme a las disposiciones del Código de la Niñez y Adolescencia y demás normativa vigente. De identificarse aquello, el consentimiento obtenido será considerado inválido.

- Visitantes del sitio web

Cuando visita nuestro sitio web, utilizamos cookies para que el sitio web funcione, y los datos solicitados por la compañía son recogidos conforme el punto 8.1.

- Comunicación con clientes potenciales.

Cuando tenga preguntas sobre nuestro sitio web o desee obtener más información sobre nuestros servicios, puede contactarnos a través de:

- Formulario de contacto

- Correo electrónico
- Teléfono

Con estos medios, trataremos su información personal para entablar un diálogo con usted, por ejemplo, responder preguntas sobre nuestros servicios. Solo tratamos la información que nos proporciona en relación con nuestra comunicación.

Por lo general, trataremos la siguiente información general:

- nombre
- correo
- electrónico
- número de teléfono.

9. MEDIDAS DE SEGURIDAD

La Empresa implementará medidas de seguridad técnicas, físicas y organizativas para proteger los datos personales, incluyendo:

9.1. Principio de Seguridad

La Empresa implementará medidas de seguridad técnicas, físicas y organizativas para proteger los datos personales. El responsable o encargado del tratamiento de datos personales deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo con la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.

Entre otras medidas, se podrán incluir las siguientes:

- Medidas de anonimización, seudonimización o cifrado de datos personales.

- Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes.

- Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, y jurídica.

- Los responsables y encargados del tratamiento de datos personales podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la

información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

Para ello, la Empresa implementará:

- **Protección antivirus:** Implementación de software antivirus en todos los dispositivos que manejen datos personales.
- **Respaldo de información:** Realización de copias de seguridad periódicas para prevenir la pérdida de datos.
- **Eliminación segura de datos:** Implementación de procesos para la eliminación segura de datos personales cuando ya no sean necesarios.
- **Control de acceso:** Restricción del acceso a los datos personales únicamente a las personas autorizadas.

9.2. Protección de Datos desde el Diseño y por Defecto

La Empresa, como responsable del tratamiento, tiene el deber de tener en cuenta, en las primeras fases de concepción y diseño de proyectos, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento.

Asimismo, la Empresa aplicará las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento. Además, mediante los respectivos ajustes, las medidas deben garantizar que por defecto, los datos no puedan ser accesibles a un número indefinido de personas de forma automatizada.

9.3. Evaluación de Impacto del Tratamiento de Datos Personales (EIPD)

La Empresa realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera.

La evaluación de impacto relativa a la protección de los datos será de carácter obligatoria en caso de:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración

de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales.

- Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales.

- Observación sistemática a gran escala de una zona de acceso público.

La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales. En caso de duda, la Empresa podrá dirigir una consulta a la Autoridad de Protección de Datos Personales con la finalidad de que determine la obligatoriedad de la evaluación de impacto. La evaluación de impacto contendrá, al menos: la descripción sistemática de las operaciones de tratamiento y sus finalidades; la justificación de la necesidad y proporcionalidad; la evaluación de riesgos a los derechos y libertades; y las medidas previstas para hacer frente a los riesgos, garantías y mecanismos de seguridad.

9.4. Notificación de Vulneración de Seguridad

El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación.

El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.

El responsable del tratamiento deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, dentro del término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo. No se deberá notificar la vulneración de seguridad de datos personales al titular en los siguientes casos:

- Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas organizativas o de cualquier otra índole apropiadas aplicadas a los datos personales afectados por la vulneración de seguridad que se pueda demostrar que son efectivas.

- Cuando el responsable del tratamiento haya tomado medidas que garanticen que el riesgo para los derechos fundamentales y las libertades individuales del titular no ocurrirá.

- Cuando se requiera un esfuerzo desproporcionado para hacerlo; en cuyo caso, el responsable del tratamiento deberá realizar una comunicación pública a través de cualquier medio en la que se informe de la vulneración de seguridad de datos personales a los titulares.

La notificación de vulneración de seguridad deberá contener: la naturaleza y tipo de vulneración; identificar los titulares afectados; el detalle inicial de los sistemas vulnerados; la causa presunta de la vulneración; el volumen y tipos de datos expuestos o comprometidos; las medidas adoptadas y previstas para responder y remediar la vulneración; y la evaluación del riesgo que la vulneración implica para los derechos y libertades de los titulares.

10. CAPACITACIÓN

La Empresa realizará capacitaciones anuales a su personal sobre los principios, derechos y obligaciones establecidos en la Ley Orgánica de Protección de Datos Personales. Estas capacitaciones incluirán:

- Concienciación sobre la importancia de la protección de datos personales.
- Formación en el manejo seguro de la información.
- Actualización sobre cambios en las normativas de protección de datos.

La Empresa, como responsable y encargado del tratamiento de datos personales, deberá capacitar y actualizar a su Delegado de Protección de Datos Personales, de conformidad con la normativa técnica que emita la Autoridad de Protección de Datos Personales.

11. RELACIÓN CON LA AUTORIDAD DE CONTROL

11.1. Delegado de Protección de Datos Personales (DPO)

La Empresa mantendrá un diálogo fluido con la Autoridad de Protección de Datos. Se designará un Delegado de Protección de Datos Personales en los siguientes casos:

- Cuando el tratamiento se lleve a cabo por quienes conforman el sector público.

- Cuando las actividades del responsable o encargado del tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento, conforme se establezca en la LOPDP, su reglamento, o en la normativa que dicte al respecto la Autoridad de Protección de Datos Personales.

    - Para determinar si las actividades requieren un control permanente, se considerará: si el tratamiento de datos es continuado o en intervalos concretos durante un tiempo; si es recurrente o repetido en momentos prefijados; o si tiene lugar de manera constante o periódica.

- Para determinar si el control es sistematizado, se verificará: si el tratamiento de datos está preestablecido, organizado o es metódico; si tiene lugar como parte de un plan general de recogida de datos; o si es llevado a cabo como parte de una estrategia.

- Cuando se refiera al tratamiento a gran escala de categorías especiales de datos, de conformidad con lo establecido en el reglamento de la LOPDP.

- Cuando el tratamiento no se refiera a datos relacionados con la seguridad nacional y defensa del Estado que adolezcan de reserva ni fuesen secretos.

El DPO será responsable de:

1. Asesorar al responsable, al personal del responsable y al encargado del tratamiento de datos personales, sobre las disposiciones contenidas en la LOPDP, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales.

2. Supervisar el cumplimiento de las disposiciones contenidas en la LOPDP, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales.

3. Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación.

4. Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales.

5. Las demás que llegase a establecer la Autoridad de Protección de Datos Personales con ocasión de las categorías especiales de datos personales.

Para ser Delegado de Protección de Datos Personales, se requerirá, entre otros, estar en goce de los derechos políticos, ser mayor de edad, tener título de tercer nivel en Derecho, Sistemas de Información, Comunicación, o de Tecnologías; y acreditar experiencia profesional de por lo menos cinco años. No podrán ser delegados quienes formen parte de los órganos de administración y control del responsable y encargado; los socios o accionistas del responsable y encargado; los cónyuges de los administradores, directores o comisarios de la compañía, en caso de haberlos, del responsable y encargado, o sus parientes hasta el cuarto grado de consanguinidad o segundo de afinidad; y quienes tengan conflictos de intereses con el responsable y encargado.

11.2. Registro de Actividades de Tratamiento

La Empresa, si cuenta con cien o más trabajadores, llevará un registro de todas las actividades de tratamiento de datos personales que sean de su competencia. Este registro contendrá la siguiente información:

- El nombre y los datos de contacto del responsable del tratamiento y, en su caso, del responsable que actúa conjuntamente, así como el nombre y los datos de contacto del delegado de protección de datos.
- Los fines del tratamiento.
- Las categorías de destinatarios a los que se han comunicado o se comunicarán los datos personales.
- Identificar a los titulares y las categorías de datos personales de los titulares.
- En su caso, el uso de perfiles.
- En su caso, definir las transferencias de datos personales a organismos de un tercer país o a una organización internacional.
- Descripción de las bases legitimadoras que facultan el tratamiento.
- Los plazos de retención previstos para la supresión o la revisión de la necesidad de conservar las diferentes categorías de datos personales.
- Una descripción general de las medidas técnicas, jurídicas, administrativas y organizativas.

La obligación de registro de actividades también la tendrán los responsables de tratamiento que, teniendo menos de cien trabajadores, cumplan alguna de las siguientes condiciones:

El tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los titulares.

No se trate de un tratamiento ocasional.

Incluya categorías especiales de datos personales.

12. APROBACIÓN Y ENTRADA EN VIGOR

Este Manual será comunicado a todas las personas relacionadas con la Empresa y será revisado periódicamente para asegurar su cumplimiento con las normativas vigentes. La Empresa se compromete a actualizar este Manual en caso de cambios en las leyes o regulaciones aplicables.

Referencias:

- Ley Orgánica de Protección de Datos Personales (Quinto Suplemento del Registro Oficial No. 459, 26 de mayo de 2021).
- Reglamento General de la Ley Orgánica de Protección de Datos Personales (Decreto No. 904, Tercer Suplemento del Registro Oficial No. 435, 13 de noviembre de 2023).
- Resolución No. 013-DN-DINARP-2021 (Registro Oficial No. 567, 27 de octubre de 2021).
- Norma ISO 27001:2013 (Gestión de la Seguridad de la Información).
- Norma ISO 9001:2015 (Gestión de la Calidad).
- Norma ISO 20000-1:2018 (Gestión de Servicios de TI).

SILVIA DEL ROCIO ITURRALDE ESCOBAR

Firmado digitalmente por SILVIA DEL ROCIO ITURRALDE ESCOBAR
Fecha: 2025.07.21 13:13:45 -05'00'

_____

Firma de Aprobación:
Mgs. Silvia del Rocío Iturralde Escobar
Presidente Ejecutivo de Cámara
01 de abril del 2025

_____

Este Manual de Privacidad y Políticas de Protección de Datos Personales es un documento vivo que se actualizará según sea necesario para garantizar el cumplimiento continuo con las normativas aplicables y las mejores prácticas en materia de protección de datos.