

## POLÍTICA DE PRIVACIDAD DE SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.



SECURITY DATA de conformidad con las disposiciones de la Ley Orgánica de Protección de Datos Personales, publicada en el quinto Suplemento del Registro Oficial No. 459, de 26 de mayo de 2021, y demás normativa conexas en materia de protección de datos vigente en Ecuador, informa los términos y condiciones de privacidad de datos personales, así como las políticas y prácticas de protección de datos personales, uso de cookies y spam del sitio web de la compañía SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. (en adelante "SECURITY DATA"), al que se accede por medio de la URL "[https:// www.securitydata.net.ec/](https://www.securitydata.net.ec/)" y sus dominios de nivel inferior (el "sitio web" o la "página web").

Revise atentamente estos términos y condiciones, ya que le servirán para comprender las actividades, alcance del tratamiento de datos personales que realiza SECURITY DATA, así como sus finalidades, a fin de que comparta su información personal con nosotros. Estos términos y condiciones se aplican solo a la información recopilada a través de la página web.

### 1. Desarrollo.

#### 1.1 Alcance.

Este documento contiene la Política de Privacidad que SECURITY DATA implementa en la prestación de los servicios de certificación para los que se encuentra acreditada, dentro de la infraestructura Oficial de Firma Electrónica en Ecuador, de acuerdo a la regulación aplicable.

En consecuencia, la presente política será de cumplimiento obligatorio para todo el personal y/o cualquier tercero que intervenga o participe en la ejecución de las actividades relacionadas con la prestación de los servicios de certificación para los que se encuentra acreditada.

#### 1.2 Objetivos.

##### 1.2.1 General.

Desarrollar lineamientos que permitan la aplicación de protección de datos personales que sean responsabilidad de SECURITY DATA, para dar cumplimiento con lo establecido en la Ley Orgánica de Protección de Datos Personales.

### 1.2.2 Específicos.

- Definir actividades a ejecutar para garantizar la protección de datos personales que sea responsabilidad de SECURITY DATA.
- Definir responsables de la ejecución de actividades definidas para garantizar la protección de datos personales que sean responsabilidad de SECURITY DATA.

### 1.3 Documentación legal de referencia.

- Constitución de la República del Ecuador
- Ley Orgánica de Protección de Datos Personales
- Reglamento a la Ley Orgánica de Protección de Datos Personales

## 2. Términos y Definiciones.

Para efectos del presente documento, se aplicarán las siguientes definiciones, las cuales se encuentran establecidas en el artículo 4 de la LPDP.

**Autoridad de Protección de Datos Personales:** Autoridad pública independiente encargada de supervisar la aplicación de la presente Ley, reglamento y resoluciones que ella dicte, 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.

**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.

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

**Dato biométrico:** Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.

**Dato genético:** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.

**Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

**Datos personales crediticios:** Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.

**Datos relativos a:** etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos, datos relativos a las personas apátridas y refugiados que requieren protección internacional, y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

**Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

**Datos sensibles:** 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:** 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, Habilidad, 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.

**Entidad Certificadora:** Entidad reconocida por la Autoridad de Protección de Datos P Personales, que podrá, de manera no exclusiva, proporcionar certificaciones en materia de protección de datos personales.

**Fuente accesible al público:** Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.

**Responsable de tratamiento de datos personales:** persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

**Sellos de protección de datos personales:** Acreditación que otorga la entidad certificadora al responsable o al encargado del tratamiento de datos personales, de haber implementado mejores prácticas en sus procesos, con el objetivo de promover la confianza del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

**Seudonomización:** 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.

**Transferencia o comunicación:** Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comuniquen deben ser exactos, completos y actualizados.

**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.

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

### 3. Principios del tratamiento de datos personales.

Se considerará el tratamiento de datos personales, respetando las normas generales y especiales sobre la materia. El desarrollo, interpretación y aplicación de la presente política, se aplicará lo estipulado en la LOPDP, en el artículo 10.

- a) **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 presente Ley, su Reglamento y la demás normativa y jurisprudencia aplicable.

- b) 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.
- c) 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.  
Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia.
- d) 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 esta Ley.  
El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.
- e) 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.
- f) 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.
- g) 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 esta Ley.  
Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio.

**h) 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.

Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales. Siempre que el responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, no le será imputable la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del titular.

b) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable.

c) Fuesen obtenidos de un registro público por el responsable.

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

Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica.

La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias, para salvaguardar los derechos previstos en esta norma.

**j) 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.

**k) 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 presente Ley, 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.

El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales.

El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley.

**l) 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.

**m) Independencia del control.** - Para el efectivo ejercicio del derecho a la protección de datos personales, y en cumplimiento de las obligaciones de protección de los derechos que tiene el Estado, la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción.

#### **4. Información Recopilada.**

La recogida y tratamiento automatizado de los datos de carácter personal tiene como finalidad el mantenimiento de la relación comercial y el desempeño de tareas de información, formación, asesoramiento y otras actividades propias de SECURITY DATA.

Estos datos únicamente serán compartidos a aquellas entidades que sean necesarias con el único objetivo de dar cumplimiento a la finalidad anteriormente expuesta.

##### **4.1 ¿Cuál es la información que recopilamos?**

###### **Datos que nos ha facilitado directamente el cliente**

Para efectuar la comercialización de nuestros productos y servicios requerimos de sus datos personales, los mismos que nos ha facilitado al momento de adquirir nuestros servicios y/o productos; nos ha otorgado a través de los formularios del sitio web; o, a través del centro de servicio al cliente.

Los datos personales facilitados por el cliente de manera directa, de manera no limitativa son: nombres y apellidos, dirección de correo

electrónico, número de teléfono, reclamos o requerimientos, etc., así como cualquier otro tipo de información facilitada durante el transcurso de la relación comercial.

### **Datos recabados de forma automatizada**

Recabamos datos de forma automatizada cuando visita o navega única y exclusivamente por nuestro sitio web (<https://www.securitydata.net.ec/>), a través de cookies (pequeños archivos de texto almacenados en su navegador), utilizando Google Analytics, de la cual no podemos identificar la identidad del usuario. Estos datos son: Número de visitas, Tiempo de navegación, Tipo de navegador, Información de tracking, Servicio revisado o de interés. Esta opción es aplicable y parametrizable dependiendo de la configuración de su navegador.

### **Datos obtenidos de fuentes externas**

Adicionalmente, información subida voluntariamente por el usuario a distintas plataformas de redes sociales los profesionales como facebook, twitter y demás, en las cuales ha aceptado de antemano las políticas, las condiciones propias de cada plataforma, todo ello con el fin de analizar intereses y las preferencias de sus clientes.

### **Datos derivados de la adquisición de un Servicio de SECURITY DATA**

Corresponde a datos necesarios para que, de acuerdo a la normativa tributaria ecuatoriana vigente, cumplamos con el proceso de facturación, así como para la prestación adecuada del servicio contratado, referente al tipo de servicios elegidos, datos de facturación, y demás relacionados a la gestión de cobranza la facturación.

## **5. Derechos de los titulares de los datos.**

Las personas que autorizan el tratamiento de datos personales, son titulares de los derechos previstos en el capítulo III de la LOPDP.

### **5.1 Derecho de acceso.**

El titular de los datos tiene la potestad de acceder a la totalidad de su información personal en posesión del responsable del tratamiento, así como a los detalles especificados en el artículo precedente. Este acceso se garantiza de forma gratuita y no requiere justificación alguna por parte del titular.

El responsable del tratamiento tiene la obligación de implementar mecanismos expeditos y razonables para facilitar el ejercicio de este derecho, debiendo atender las solicitudes en un plazo máximo de quince (15) días.

Es importante destacar que el ejercicio de este derecho de acceso no podrá constituir un abuso del mismo.

## **5.2 Derecho de rectificación y actualización.**

En virtud de su derecho, el titular de los datos personales podrá requerir la rectificación y actualización de cualquier información que sea inexacta o esté incompleta. Para tal efecto, deberá diligenciar y presentar el Formulario SOLICITUD DE DERECHOS DE TITULARES DE DATOS PERSONALES que se encuentra en:

[https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/Formulario\\_Derechos\\_Titulares\\_Dato\\_Personal.pdf](https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/Formulario_Derechos_Titulares_Dato_Personal.pdf)

adjuntando la documentación justificativa que corresponda. La tramitación y respuesta a la solicitud se efectuará en un plazo no superior a quince (15) días contados desde su recepción.

## **5.3 Derecho de eliminación.**

El titular de datos podrá solicitar a SECURITY DATA, la eliminación de sus datos en los casos contemplados en el artículo 15 de la LOPDP.

Con excepción de lo manifestado en el artículo 18 del mismo cuerpo normativo. La tramitación y respuesta a la solicitud se efectuará en un plazo no superior a quince (15) días contados desde su recepción.

## **5.4 Derecho de oposición.**

El titular de datos podrá solicitar a SECURITY DATA, a la oposición de sus datos en los casos contemplados en el artículo 16 de la LOPDP.

Con excepción de lo manifestado en el artículo 18 del mismo cuerpo normativo. La tramitación y respuesta a la solicitud se efectuará en un plazo no superior a quince (15) días contados desde su recepción.

## **5.5 Derecho a la portabilidad.**

El titular de datos personales ostenta el derecho, conforme al Artículo 17 de la LOPDP, a recibir del responsable del tratamiento sus datos personales en un formato compatible, actualizado, estructurado, de uso común, interoperable y de lectura mecánica, garantizando la preservación de sus características originales. Asimismo, se faculta al titular a transmitir dichos datos a otros responsables. La Autoridad de Protección de Datos Personales será la entidad encargada de dictar la normativa específica para el adecuado ejercicio de este derecho a la portabilidad.

El titular podrá solicitar al responsable del tratamiento la transferencia o comunicación directa de sus datos personales a otro responsable, siempre que ello sea técnicamente factible. El responsable originario no podrá invocar

impedimento alguno que retarde o dificulte el acceso, la transmisión o la reutilización de los datos por parte del titular o de otro responsable del tratamiento.

Una vez completada la transferencia de los datos, el responsable que la ha efectuado deberá proceder a la eliminación de la información, a menos que el titular disponga su conservación. El responsable que reciba la información transferida asumirá plenamente las responsabilidades y obligaciones establecidas en la presente Ley.

Para que proceda dicho derecho, deberá observarse las condiciones establecidas en el artículo 17:

- a) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. La transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible; en caso contrario los datos deberán ser transmitidos directamente al titular.
- b) Que el tratamiento se efectúe por medios automatizados;
- c) Que se trate de un volumen relevante de datos personales, según los parámetros definidos en el reglamento de la presente Ley; o,
- d) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social.

Esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita y sin trabas.

El derecho de portabilidad no será aplicable a la información que haya sido inferida, derivada, creada, generada u obtenida como resultado del análisis o tratamiento efectuado por el responsable de los datos personales, cuando dicho proceso se base en los datos personales inicialmente proporcionados por el titular. Esto incluye, a modo de ejemplo, los datos personales que hayan sido objeto de personalización, recomendación, categorización o creación de perfiles.

## **5.6 Derecho a la suspensión del tratamiento.**

El titular de datos podrá solicitar a SECURITY DATA, la suspensión del tratamiento de sus datos en los casos contemplados en el artículo 19 de la LOPDP.

- a) Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos;
- b) El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
- c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y,

- d) Cuando el interesado se haya opuesto al tratamiento en virtud del artículo 31 de la presente Ley, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

### **5.7 Derecho a no ser objeto de una decisión basada única o parcialmente en valoración automatizadas.**

El titular de los datos, tendrá derecho a lo estipulado en el artículo 20 de la LOPDP, considerando que tendrá la posibilidad de:

- a) Solicitar al responsable del tratamiento una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos personales;
- b) Presentar observaciones;
- c) Solicitar los criterios de valoración sobre el programa automatizado; o,
- d) Solicitar a la responsable información sobre los tipos de datos utilizados y la fuente de la cual han sido obtenidos los mismos;
- e) Impugnar la decisión ante el responsable o encargado del tratamiento

No se aplicará este derecho cuando:

- a) La decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos personales;
- b) Está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad técnica competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; o,
- c) Se base en el consentimiento explícito del titular.
- d) La decisión no conlleve impactos graves o riesgos verificables para el titular.

### **5.8 Derecho de consulta.**

Toda persona tiene derecho a consultar de forma pública y gratuita el Registro Nacional de Protección de Datos Personales, en estricta conformidad con lo dispuesto en la presente Ley.

### **5.9 Derecho a la educación digital.**

Toda persona ostenta el derecho fundamental al acceso y disponibilidad al conocimiento, aprendizaje, preparación, estudio, formación, capacitación, enseñanza e instrucción relativos al uso y manejo adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación (TIC). Este derecho se ejercerá en estricto apego a la dignidad e integridad humana, a los derechos fundamentales y libertades individuales, con especial énfasis en la intimidad, la vida privada, la autodeterminación informativa, la identidad y reputación en línea, la ciudadanía digital y el derecho a la protección de datos personales. Asimismo, se promoverá una cultura sensibilizada respecto al derecho a la protección de datos personales.

El derecho a la educación digital tendrá un carácter inclusivo, prestando especial atención a las personas con necesidades educativas especiales.

El sistema educativo nacional, incluyendo el sistema de educación superior, garantizará la educación digital no solo en beneficio de los estudiantes de todos los niveles, sino también de los docentes, debiendo integrar dicha temática en sus respectivos procesos de formación.

## **6. Finalidades de la información.**

Los datos personales facilitados por el cliente serán utilizados por SECURITY DATA para gestionar adecuadamente los servicios solicitados o contratados, y en los términos informados en la presente política de privacidad y sus actualizaciones, conforme a las siguientes bases de legitimidad:

- Finalidades basadas en el cumplimiento de la relación comercial y la ejecución del contrato de servicios:

Aquellas necesarias para llevar a cabo la venta de los servicios de SECURITY DATA, y la gestión de la relación a efectos de dar cumplimiento a lo dispuesto a las transacciones comerciales, como las que se detallan a continuación:

- Gestionar, tramitar y dar respuesta a peticiones, solicitudes, incidencias o consultas del usuario, cuando éste facilite sus datos a través de los formularios habilitados en el sitio web <https://www.securitydata.net.ec/> o a través de nuestros medios de centros de atención al cliente.
- Gestionar la confirmación de la identidad y datos civiles de los potenciales clientes, en base a la información procedente del Registro Civil, Identificación y Cedulación, la Dirección Nacional de Registros Públicos (DINARDAP) y Servicio de Rentas Internas (SRI) Superintendencia de compañías, entre otros.
- Analizar los requerimientos realizados por los Organismos de Control, entes regulatorios, fiscalía u órdenes judiciales, que permita mantener la seguridad de las transacciones, revisión de eventos ilegales o fraudulentos.
- De forma periódica, SECURITY DATA envía encuestas de evaluación, con el fin de mejorar la satisfacción del cliente en función de sus necesidades, para mantener la fidelización de nuestros clientes, o cuando ha existido inconvenientes técnicos para poder garantizar la calidad del servicio al cliente recibido por nuestros vendedores.

- Finalidades basadas en el consentimiento del Titular de Datos Personales:

Son aquellos asumidos por las partes en base a las obligaciones mutuas que han adquirido, en relación a los productos y/o servicios ofrecidos por SECURITY DATA:

- En caso de impago, podremos comunicar sus datos personales asociados a una obligación pendiente, a los organismos auxiliares del sistema financiero y/o a las entidades responsables de dichos sistemas de información crediticia para su publicación en los ficheros de solvencia, ante cualquier institución debidamente acreditada.
- Efectuar encuestas de satisfacción y estudios de mercado que tengan como finalidad conocer las preferencias e intereses comerciales de los clientes.
- Para analizar sus preferencias utilizamos los datos derivados de la venta, consumo y facturación media de los Servicios, que formen parte de las ventas. SECURITY DATA podrá realizar análisis sobre los datos disponibles del cliente durante la vida de la relación comercial, para diseñar un perfil (ARQUETIPO) más adaptable al cliente que permita a la empresa servirlo de mejor forma y de acuerdo a sus preferencias, el mismo incluye: estimaciones sobre el canal de compra preferido, satisfacción del servicio, la edad y género, y datos sobre sus preferencias obtenidas de las plataformas mencionadas.
- Tratamientos de anonimización de datos (proceso de convertir los datos en una forma en que no se pueda identificar a individuos) o conjuntos de datos, mediante herramientas que permitan obtener resultados agregados, con el fin de realizar estimaciones con fines estadísticos, de interés público o de investigación científica o histórica.
- Para realizar tratamiento de los datos personales del cliente y/o potencial cliente, a fin de ejecutar las relaciones contractuales que mantenga vigentes o que pueda sostener en el futuro con SECURITY DATA, así como para fines estadístico los/o analítico los/o para que se evalúe la calidad del servicio brindado, atender los requerimientos los/o comunicaciones a través de los canales de atención de SECURITY DATA.
- Para permitir el envío de comunicaciones comerciales por parte de SECURITY DATA ajustadas a tu “arquetipo” sobre propio los/o de terceros con los cuales SECURITY DATA mantiene alianzas

- estratégicas para brindar beneficios.
- Para realizar el tratamiento de los datos personales, así como datos de imagen y video, que se obtengan y/o se suministren por personas que asistan a eventos organizados por SECURITY DATA, para efectuar campañas publicitarias los promocionales a través de publicaciones en redes sociales como Facebook, Instagram, Twitter, YouTube, LinkedIn y el sitio web institucional.
  - Para prestar y personalizar las funciones de las aplicaciones los sitios web de SECURITY DATA.
  - Para analizar, diseñar, desarrollar, implementar, optimizar o realizar mantenimiento de cualquier clase de programas, aplicaciones; y, en general, cualquier software tecnológico a fin de proporcionar a los clientes y potenciales clientes una experiencia personalizada e intuitiva en las plataformas digitales de SECURITY DATA.
  - Finalidades en cumplimiento de una obligación legal:
  - Cualquier obligación de carácter legal que resulte de aplicación de las leyes, como las derivadas de obligaciones judiciales, servicios de emergencias, y demás tipificados en las normas ecuatorianas.

## **6.1 Base legal para el tratamiento.**

El titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparencia por cualquier medio.

El tratamiento legítimo de datos personales se fundamenta, primordialmente, en el consentimiento expreso e inequívoco del titular. No obstante, de conformidad con lo establecido en el artículo 7 de la Ley Orgánica de Protección de Datos Personales (LOPD), la licitud del tratamiento podrá derivarse, según el caso particular, de cualquiera de las siguientes bases jurídicas:

1. El consentimiento libre, específico, informado e inequívoco del titular de los datos.
2. Cuando el tratamiento sea necesario para el cumplimiento de una obligación legal que incumba al responsable del tratamiento.
3. Para la ejecución de una orden judicial o resolución administrativa debidamente motivada y emitida por autoridad competente.
4. El tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. Dicha potestad deberá derivar de una norma con rango de ley, y su ejercicio estará supeditado al cumplimiento de los estándares internacionales de derechos humanos aplicables en la materia, así como a la observancia de los

principios de la LOPDP y a los criterios de legalidad, proporcionalidad y necesidad.

5. Para la ejecución de medidas precontractuales adoptadas a petición del titular del dato o para el cumplimiento de obligaciones contractuales de las que sea parte el responsable del tratamiento de datos personales, el encargado del tratamiento de datos personales o un tercero legalmente habilitado.
6. Cuando el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona natural, tales como su vida, salud o integridad física.
7. El tratamiento de datos personales que consten en bases de datos de acceso público, en los términos y condiciones establecidos por la normativa aplicable.
8. Para la satisfacción de un interés legítimo del responsable del tratamiento o de un tercero, siempre y cuando no prevalezcan los derechos y libertades fundamentales de los titulares que requieran protección de datos personales, conforme a lo dispuesto en la presente normativa.

**Tipos de tratamiento.** - los datos recogidos serán tratados de manera manual y automatizada de ser el caso.

**Tiempo de conservación.** - El tratamiento de los datos personales se limitará al período estrictamente necesario para el cumplimiento de las finalidades para las cuales fueron recabados. Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento.

**Existencia de una base de datos en la que consten sus datos personales.** SECURITY DATA almacena los datos en una base de datos denominada "Clientes", misma que será conservada conforme el servicio a prestar como parte de la relación contractual hasta el cese de la misma, y serán conservados por el tiempo necesario para cumplir con las finalidades establecidas en el presente instrumento, así como en la normativa que regula a las Entidades de Certificación.

**Consecuencia para el titular de los datos personales de su entrega o negativa a ello.** - Se informa que la omisión o el suministro parcial de los datos personales requeridos impedirá la correcta prestación de los servicios solicitados, incluyendo, pero no limitándose a, la validación necesaria para el titular de los datos. Esta situación podría afectar la calidad o la viabilidad del servicio ofrecido.

**El origen de los datos personales cuando no se hayan obtenido directamente del titular.** - La recolección de determinados datos personales se efectúa a partir de fuentes de acceso público, bases de datos de dominio público o entidades de la administración pública, en estricto cumplimiento de la normativa vigente.

**Efecto de suministrar datos personales erróneos o inexactos.** - La inexactitud o falta de veracidad en los datos proporcionados impedirá garantizar la eficiente prestación del servicio al respectivo titular. Ello podría conducir a que las determinaciones fundamentadas en dicha información carezcan de precisión y fiabilidad, como resultado de la deficiente calidad de la información entregada.

**La posibilidad de revocar el consentimiento.** – El consentimiento otorgado por el titular de los datos personales podrá ser revocado, siempre que así lo permitan las disposiciones pertinentes de la Ley Orgánica de Protección de Datos Personales (LOPDP).

## **7. Transferencia de Datos.**

### **Transferencia o comunicaciones, nacionales o internacionales.**

SECURITY DATA podrá realizar transferencias de datos personales, nacionales, con el objetivo de cumplir su objeto social, actividades de responsabilidad social y aplicación de herramientas tecnológicas. En caso de transferencia internacional, SECURITY DATA se cerciorará que sea efectuada a jurisdicciones que tutelen la protección y privacidad de datos personales.

Los destinatarios estarán sujetos a las mismas obligaciones, las medidas de seguridad, técnica y legales descritas en la Ley Orgánica de Protección de Datos Personales y la demás normativa conexas.

## **8. ¿Utilizamos cookie u otras tecnologías de seguimiento?**

Las cookies son pequeños archivos de datos que se envían a su navegador o software relacionado desde un servidor web y se almacenan en su computadora o dispositivo. Las cookies tienen como finalidad rastrear y almacenar las preferencias de los usuarios mientras usan el sitio web, así como información técnica sobre su uso del sitio web.

Como se mencionó anteriormente, en el apartado 1, el sitio web y sus sub sitios recopilan registros anónimos durante las visitas de los usuarios. Esto se puede hacer a través de cookies o tecnologías similares para retener información sobre el número de visitas, tiempo de navegación, tipo de navegador, información de tracking y servicio revisado o de interés.

## **9. Conservación de la información.**

SECURITY DATA tratará los datos personales del cliente dando cumplimiento al principio de limitación del plazo de conservación establecido en la Ley Orgánica de Datos Personales.

SECURITY DATA actuará como responsable del tratamiento de los datos personales proporcionados por el cliente, los datos proporcionados serán almacenados por SECURITY DATA.

## **10. Identidad y datos de contacto del responsable del tratamiento de datos personales.**

**Domicilio legal:** C.C. El Bosque, Alonso de Torres y Edmundo Carvajal. Oficinas Administrativas, Piso 1, oficina C8 de la ciudad de Quito.

En caso de requerir comunicarse con el delegado de Protección de Datos de SECURITY DATA enviar un correo electrónico a la siguiente dirección de contacto: [delegadodatos@securitydata.net.ec](mailto:delegadodatos@securitydata.net.ec) , sin perjuicio de los procedimientos que hubiere lugar ante la Autoridad Nacional de Protección de Datos Personales. Los datos se almacenarán en una base de datos denominada “Clientes”, misma que será conservada conforme el servicio a prestar como parte de la relación contractual hasta el cese de la misma, y serán conservados por el tiempo necesario para cumplir con las finalidades establecidas en el presente instrumento, así como en la normativa que regula a las Entidades de Certificación.

En caso de que no tenga un vínculo comercial con SECURITY DATA, la autorización brindada perdurará hasta por dos (2) años desde que otorga su consentimiento. En dicho caso, los Datos Personales serán almacenados en la base de datos de SECURITY DATA, con domicilio legal en C.C. El Bosque, Alonso de Torres y Edmundo Carvajal. Oficinas Administrativas, Piso 1, oficina C8 de la ciudad de Quito.

En caso de requerir comunicarse con el delegado de Protección de Datos de SECURITY DATA enviar un correo electrónico a la siguiente dirección de contacto: [delegadodatos@securitydata.net.ec](mailto:delegadodatos@securitydata.net.ec), sin perjuicio de los procedimientos que hubiere lugar ante la Autoridad Nacional de Protección de Datos Personales. La información se almacenará con la denominación “Potenciales Clientes”.

El titular de los datos personales proporcionará los mismos de manera personal o a través de su representante legal por medio del formulario web o virtual habilitado para el efecto.

En ambos casos, el tiempo de conservación de los datos personales suministrados por los “Potenciales clientes” o por “clientes” podrá subsistir durante el tiempo necesario según los plazos de prescripción previstos en la legislación vigente para el ejercicio o defensa de posibles reclamaciones administrativas, tributarias, legales o judiciales. En estos casos, la información se mantendrá debidamente bloqueada con acceso restringido a determinados perfiles, con las medidas técnicas y organizativas necesarias que garanticen la seguridad de la información, evitando su alteración, pérdida, tratamiento o acceso no autorizado;

transcurridos dichos plazos, los datos serán eliminados o anonimizados, según proceda, y de conformidad con la normativa ecuatoriana que resulte de aplicación.

En los casos en que obtenemos datos automáticamente a través de la navegación en nuestra página web (<https://www.securitydata.net.ec/>), el cliente podrá limitar su uso en el tiempo eliminándolas de los navegadores o dispositivos.

En caso de mantener obligaciones pendientes, podremos comunicar tus datos personales asociados a una obligación pendiente, a los organismos auxiliares del sistema financiero, hasta que las obligaciones sean cubiertas en su totalidad.

## **11. Seguridad de la Información.**

SECURITY DATA implementará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para la protección de los datos personales que le proporcionen; y, en caso de que se produzca una violación de la seguridad que dé lugar a la destrucción, pérdida o alteración accidental o ilícita, o a la divulgación o el acceso no autorizados a los datos personales proporcionados por los usuarios, SECURITY DATA lo notificará en un término máximo de tres días, contados a partir de que tuvo conocimiento de la misma.

## **12. ¿Qué pasa si no quiero compartir mi información?**

El llenado de sus datos en los formularios en nuestra página es voluntario, y sin hacerlo, los usuarios pueden navegar en la página web. Llenar los formularios es necesario para recibir información relacionada con los servicios de SECURITY DATA, sus eventos, capacitaciones y otras actividades.

Al navegar en la página web, se recopilará la información anónima descrita en el numeral 1, que, al ser anónima, no permite identificar usuarios específicos.

## **13. ¿Recolectamos información de menores de edad?**

El sitio web no está dirigido a menores de edad y no recopilamos ni conservamos ninguna información personal sobre personas menores de edad.

## **14. Identificación de personas encargadas para la atención de requerimientos**

- Responsable del tratamiento de datos personales: SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.
- Domicilio: C.C. El Bosque, Alonso de Torres y Edmundo Carvajal. Oficinas Administrativas, Piso 1, oficina C8 de la ciudad de Quito.
- Delegado de Protección de Datos (DPO): El usuario puede contactar con el delegado de datos personales (DPD) mediante escrito dirigido al domicilio de SECURITY DATA o a través del correo electrónico: [delegadodatos@securitydata.net.ec](mailto:delegadodatos@securitydata.net.ec).
- Los interesados podrán ejercer sus derechos llenando la SOLICITUD DE DERECHOS DE TITULARES DE DATOS PERSONALES que se encuentra en: [https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/Formulario\\_Derechos\\_Titulares\\_Dato\\_Personal.pdf](https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/Formulario_Derechos_Titulares_Dato_Personal.pdf), esta solicitud deberá ser entregada personalmente en cualquiera de las sucursales de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.
- Así mismo, el cliente podrá revocar en cualquier momento los consentimientos otorgados a través de nuestros centros de atención al cliente o bien a través del correo electrónico [datospersonales@securitydata.net.ec](mailto:datospersonales@securitydata.net.ec), debiendo contar con una firma electrónica o física en su requerimiento para la correspondiente autenticación.

## 15. Consentimiento.

Al utilizar nuestra plataforma y remitir sus datos personales a través de los medios dispuestos por SECURITY DATA para el efecto, expresa su consentimiento libre y voluntario a SECURITY DATA para que lleve a cabo el tratamiento de sus datos personales, de acuerdo a las finalidades, procedimiento las condiciones expresadas en nuestra Política de Privacidad; por lo cual, usted confirma que su consentimiento es específico, informado e inequívoco.

## 16. Video vigilancia.

SECURITY DATA cuenta con un sistema de video vigilancia en todas sus instalaciones a fin de garantizar la seguridad, control y supervisión de nuestro personal, visitantes, cliente proveedores/o terceros.

La administración de nuestro sistema de video vigilancia cumple con la normativa de protección de datos personales está regido por las disposiciones de esta Política, en cuanto le sean aplicables.

Asimismo, SECURITY DATA ha adoptado los niveles de seguridad y de protección de datos personales legalmente requeridos, y ha instalado todos los medios de medidas técnicas a su alcance.

La Información captada mediante nuestros sistemas de video vigilancia se encuentra gestionada en la base de datos de "Video vigilancia", y se almacenarán hasta un plazo máximo de treinta (30) días, salvo disposición distinta en normas sectoriales.

Asimismo, los datos personales se transferirán a nivel nacional a Telconet S.A. con la finalidad de Gestión de registro, procesamiento y almacenamiento de datos en la nube de SECURITY DATA. Los datos personales no se transferirán a nivel internacional.

#### **17. Actualización de los Término los Condiciones.**

La página web de SECURITY DATA se actualiza periódicamente, por lo que nuestros términos y condiciones pueden cambiar en cualquier momento. Por lo tanto, se sugiere que revise los términos y condiciones de privacidad publicados de tiempo en tiempo.

#### **18. Consulta las comunicaciones sobre los Término los Condiciones.**

Si tiene preguntas o comentarios sobre estos términos los condiciones, puede contactarnos mediante un correo electrónico a la dirección [delegadodatos@securitydata.net.ec](mailto:delegadodatos@securitydata.net.ec) o mediante una comunicación escrita dirigida C.C. El Bosque, Alonso de Torres y Edmundo Carvajal. Oficinas Administrativas, Piso 1, oficina C8 de la ciudad de Quito, o al teléfono 02-3922169.

SECURITY DATA podrá actualizar la presente Política de Privacidad en cualquier momento, respetando las obligaciones y los derechos del ordenamiento jurídico vigente, por lo cual le pedimos que revise con regularidad este documento. Dicha actualización se hará pública en cualquier caso por parte de SECURITY DATA y publicada en <https://www.securitydata.net.ec/>. Esta política tiene fecha de vigencia desde el mes de marzo del año 2023.

**Fecha de publicación:** 30 de marzo del 2023.

**Fecha de actualización:** 06 de junio del 2025.

