

1. Introducción

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A., en adelante SECURITY DATA, en cumplimiento de la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa emitida por la Superintendencia de Protección de Datos Personales, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento, la normativa sectorial aplicable a las Entidades de Certificación de Información y Servicios Relacionados Acreditadas y demás normativa vigente en el Ecuador, pone a disposición de los titulares la presente Política Publica de Protección de Datos Personales.

Esta Política tiene un carácter informativo y público. Su finalidad es comunicar los lineamientos generales bajo los cuales SECURITY DATA protege los datos personales que trata en el desarrollo de sus actividades comerciales, contractuales, administrativas, laborales, tecnológicas, regulatorias y de prestación de servicios de certificación de información, firma electrónica y servicios relacionados.

La presente Política debe interpretarse de forma armónica con la Política de Privacidad y Tratamiento de Datos Personales de SECURITY DATA, que contiene el detalle de categorías de datos, finalidades, bases de legitimación, conservación, derechos de los titulares, transferencias, seguridad, video vigilancia, cookies y demás condiciones específicas aplicables al tratamiento de datos personales.

2. Objeto

La presente Política tiene por objeto establecer y comunicar los lineamientos públicos de protección de datos personales de SECURITY DATA, orientados a garantizar que los datos personales sean tratados de forma lícita, leal, transparente, segura, confidencial, proporcional y conforme a finalidades determinadas.

En particular, esta Política busca:

- Informar a los titulares sobre los compromisos generales de SECURITY DATA en materia de protección de datos personales.
- Reforzar la transparencia respecto de la forma en que SECURITY DATA protege la información personal bajo su responsabilidad.
- Comunicar los canales disponibles para el ejercicio de derechos y contacto con el Delegado de Protección de Datos.
- Mantener coherencia con la Política de Privacidad y Tratamiento de Datos Personales vigente.
- Reconocer la calidad de SECURITY DATA como Entidad de Certificación de Información y Servicios Relacionados Acreditada.

3. Alcance

Esta Política aplica a los tratamientos de datos personales realizados por SECURITY DATA, ya sea en calidad de responsable o encargado del tratamiento, respecto de los datos de clientes, usuarios, suscriptores, solicitantes de servicios, representantes legales, administradores, apoderados, contactos técnicos, financieros o comerciales, proveedores, contratistas, aliados, trabajadores, ex trabajadores, postulantes, pasantes, visitantes, usuarios de plataformas, sitios web, aplicaciones, canales digitales y cualquier otro titular cuyos datos sean tratados por SECURITY DATA.

En especial, comprende los tratamientos relacionados con la solicitud, enrolamiento, verificación de identidad, validación documental, emisión, activación, renovación, suspensión, revocatoria, soporte, conservación y trazabilidad de certificados de firma electrónica y demás servicios de certificación de información y servicios relacionados.

4. Relación con la Política de Privacidad y Tratamiento de Datos Personales

Esta Política Publica de Protección de Datos Personales no sustituye a la Política de Privacidad y Tratamiento de Datos Personales de SECURITY DATA. Ambas forman parte del sistema documental de cumplimiento de la organización y deben leerse de manera complementaria.

La Política de Privacidad y Tratamiento de Datos Personales contiene la información específica que debe conocer el titular sobre el tratamiento de sus datos, incluyendo categorías de datos tratados, finalidades, bases de legitimación, conservación, transferencias, derechos, procedimiento de atención, cookies, video vigilancia y datos de contacto del responsable y del Delegado de Protección de Datos.

La presente Política Publica de Protección de Datos Personales resume los compromisos generales de SECURITY DATA y refuerza el marco de protección, seguridad, confidencialidad, responsabilidad proactiva, trazabilidad y cumplimiento normativo aplicable.

5. Marco normativo aplicable

Para la interpretación y aplicación de esta Política se observará, según corresponda:

- Constitución de la República del Ecuador.
- Ley Orgánica de Protección de Datos Personales y su Reglamento General.
- Resoluciones, lineamientos, guías, normas técnicas y criterios emitidos por la Superintendencia de Protección de Datos Personales.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Normativa sectorial aplicable a las Entidades de Certificación de Información y Servicios Relacionados Acreditadas.
- Disposiciones, requerimientos y actos de control emitidos por ARCOTEL en el ámbito de sus competencias.

- Normativa tributaria, societaria, laboral, administrativa, judicial, de telecomunicaciones, seguridad de la información y demás normativa aplicable al giro ordinario de SECURITY DATA.

6. Identificación del responsable y canal de contacto

Dato	Información
Responsable del tratamiento	SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.
RUC	1792261848001
Domicilio	Pichincha / Quito / Rumipamba / Alonso de Torres LC 08 S/N y Av. Del Parque
Teléfono	023922169 / 043922169
Sitio web	https://www.securitydata.net.ec/
Canal general de datos personales	datospersonales@securitydata.net.ec
Delegado de Protección de Datos	delegadodatos@securitydata.net.ec
Formulario para ejercicio de derechos	https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/Formulario_Derechos_Titulares_Dato_Personal.pdf

Cuando SECURITY DATA actué como encargado del tratamiento, tratara los datos personales conforme a las instrucciones documentadas del responsable del tratamiento y de acuerdo con el contrato, convenio, orden de servicio o instrumento jurídico aplicable.

7. Principios y compromisos de protección de datos

SECURITY DATA aplicara los principios previstos en la normativa de protección de datos personales y adoptara medidas para demostrar su cumplimiento. Entre otros, se observarán los siguientes lineamientos:

Principio o compromiso	Aplicación general
Juridicidad	Todo tratamiento deberá contar con una base de legitimación aplicable y realizarse conforme a la normativa vigente.
Lealtad y transparencia	Los titulares serán informados de manera clara, accesible y comprensible sobre el tratamiento de sus datos personales.
Finalidad	Los datos serán tratados para finalidades determinadas, explícitas, legítimas y comunicadas al titular cuando corresponda.
Minimización y proporcionalidad	Se tratarán únicamente los datos necesarios, adecuados y pertinentes para cada finalidad.
Confidencialidad	Toda persona que acceda a datos personales deberá mantener reserva y confidencialidad sobre dicha información.

Calidad exactitud y	SECURITY DATA procurara que los datos sean exactos, completos y actualizados, conforme a la finalidad del tratamiento.
Seguridad	Se aplicaran medidas técnicas, organizativas, jurídicas y administrativas razonables y proporcionales al riesgo.
Conservación	La información se conservara conforme a las finalidades informadas, obligaciones aplicables y normativa sectorial de Entidades de Certificación.
Responsabilidad proactiva	SECURITY DATA mantendrá evidencias, políticas, controles, registros, capacitaciones y mecanismos de cumplimiento.

8. Categorías generales de titulares y datos personales

SECURITY DATA podrá tratar datos personales de las siguientes categorías de titulares:

- Clientes, usuarios, suscriptores y solicitantes de servicios.
- Representantes legales, administradores, apoderados y contactos autorizados de clientes.
- Proveedores, contratistas, aliados estratégicos y sus representantes.
- Trabajadores, ex trabajadores, postulantes y pasantes.
- Visitantes de instalaciones físicas.
- Usuarios de sitios web, plataformas, aplicaciones, formularios, canales digitales o medios de atención.
- Personas naturales cuyos datos sean tratados en el marco de los servicios prestados por SECURITY DATA.

Las categorías de datos personales podrán incluir, según corresponda y de acuerdo con la finalidad aplicable: datos identificativos, datos de contacto, datos laborales o profesionales, datos contractuales y comerciales, datos financieros y de facturación, datos tecnológicos, registros de acceso, logs, metadatos, imágenes de video vigilancia, datos de trabajadores, datos sensibles cuando exista base de legitimación suficiente, datos de enrolamiento y validación de identidad, datos asociados a certificados de firma electrónica y datos obtenidos de fuentes oficiales o terceros autorizados.

SECURITY DATA tratara estas categorías de datos únicamente cuando sean necesarias, pertinentes y proporcionales para la prestación de servicios, el cumplimiento de obligaciones legales o regulatorias, la seguridad jurídica de los certificados emitidos, la trazabilidad de las operaciones y la atención de requerimientos de autoridad competente.

9. Finalidades generales del tratamiento

SECURITY DATA podrá tratar datos personales para finalidades relacionadas con:

- Gestión de solicitudes, cotizaciones, contratación, activación, renovación, suspensión, revocatoria, soporte y terminación de servicios.
- Verificación de identidad, validación documental y validación de representación o habilitación para solicitar servicios.

- Prestación de servicios de certificación de información, firma electrónica, validación de identidad, verificación de certificados y servicios relacionados.
- Administración de cuentas, perfiles, accesos, credenciales y usuarios en plataformas tecnológicas.
- Atención al cliente, soporte técnico, gestión de requerimientos, reclamos o consultas.
- Gestión contractual, comercial, operativa, administrativa, contable, tributaria y financiera.
- Cumplimiento de obligaciones legales, regulatorias, contractuales y requerimientos de autoridad competente.
- Prevención, detección y respuesta frente a incidentes de seguridad, fraude, suplantación de identidad, accesos no autorizados o uso indebido de certificados.
- Seguridad física, control de acceso, protección de personas, bienes, instalaciones, sistemas e información.
- Comunicaciones institucionales, encuestas, eventos, capacitaciones, mejoras del servicio y comunicaciones comerciales cuando exista base de legitimación aplicable.

Las finalidades específicas constan en la Política de Privacidad y Tratamiento de Datos Personales vigente de SECURITY DATA.

10. Bases de legitimación

SECURITY DATA tratará datos personales cuando exista una base de legitimación aplicable. Según el caso, el tratamiento podrá sustentarse en:

- Ejecución de medidas precontractuales o contractuales.
- Cumplimiento de obligaciones legales o regulatorias.
- Cumplimiento de requerimientos, ordenes, decisiones o actuaciones de autoridad competente.
- Interés legítimo, cuando sea permitido por la normativa aplicable y se realice la evaluación de ponderación correspondiente.
- Consentimiento del titular, cuando la normativa o la finalidad específica lo requiera.
- Otras bases reconocidas por el ordenamiento jurídico aplicable.

La prestación de servicios de certificación no se sustenta de forma general e indiscriminada en el consentimiento cuando el tratamiento sea necesario para la ejecución contractual, el cumplimiento de obligaciones legales o regulatorias, la seguridad de los servicios, la trazabilidad de los certificados o la atención de requerimientos de autoridad competente.

11. Servicios de certificación de información y firma electrónica

SECURITY DATA, en su calidad de Entidad de Certificación de Información y Servicios Relacionados Acreditada, trata determinados datos personales en el marco de la infraestructura oficial de firma electrónica en Ecuador.

En este contexto, SECURITY DATA podrá tratar datos personales para procesos de solicitud, enrolamiento, verificación de identidad, validación documental, emisión, activación, renovación, suspensión, revocatoria, soporte, conservación, trazabilidad, auditoria, control y atención de requerimientos de autoridad competente.

La información vinculada con certificados electrónicos, expedientes de identidad, registros de validación, evidencias de enrolamiento, registros de firma, declaraciones de prácticas de certificación, políticas de certificación, logs, soportes documentales y demás información necesaria para la prestación del servicio se conservará conforme a la normativa aplicable a las Entidades de Certificación y al ordenamiento jurídico vigente.

12. Conservación de la información

SECURITY DATA conservará los datos personales durante el tiempo necesario para cumplir las finalidades para las cuales fueron recolectados, así como para atender obligaciones legales, contractuales, regulatorias, contables, tributarias, laborales, societarias, administrativas, de auditoria, seguridad, trazabilidad, defensa jurídica o requerimientos de autoridad competente.

En el caso de servicios de certificación de información, firma electrónica y servicios relacionados, SECURITY DATA conservará la información durante los plazos exigidos por la normativa aplicable a las Entidades de Certificación de Información y Servicios Relacionados Acreditadas y, en particular, durante la vigencia de la acreditación, sin perjuicio de plazos adicionales que correspondan conforme al ordenamiento jurídico vigente.

Cuando el titular ejerza derechos respecto de información cuya conservación sea necesaria para cumplir obligaciones legales, regulatorias, contractuales, de auditoria, control, seguridad, trazabilidad o defensa jurídica, SECURITY DATA evaluará la solicitud y emitirá la respuesta motivada que corresponda conforme a la normativa aplicable.

13. Comunicaciones, transferencias y encargados

SECURITY DATA podrá comunicar o transferir datos personales cuando exista base de legitimación aplicable y sea necesario para cumplir finalidades informadas, obligaciones legales, regulatorias, contractuales, de auditoria, trazabilidad, seguridad, defensa jurídica o requerimientos de autoridad competente.

Los datos podrán ser comunicados, según corresponda, a autoridades administrativas, judiciales, tributarias, laborales, regulatorias o de control; ARCOTEL; Superintendencia de Protección de Datos Personales; Registro Civil; Dirección Nacional de Registros Públicos; Servicio de Rentas Internas; Superintendencia de Compañías, Valores y Seguros; proveedores tecnológicos; proveedores de nube, soporte, mantenimiento, ciberseguridad, continuidad operativa, gestión documental; entidades financieras, contables, auditoras, aseguradoras, asesoras; clientes o responsables del tratamiento cuando SECURITY DATA actué como encargado; y terceros autorizados por el titular o por la ley.



Cuando SECURITY DATA contrate encargados del tratamiento o terceros que accedan a datos personales, procurara que los contratos incluyan obligaciones de confidencialidad, seguridad, tratamiento conforme a instrucciones documentadas, gestión de incidentes, subcontratación autorizada, trazabilidad, conservación, devolución de información cuando corresponda y demás condiciones exigidas por la normativa aplicable.

SECURITY DATA no venderá ni alquilará bases de datos personales a terceros para fines comerciales ajenos a la relación contractual sin contar con una base jurídica suficiente y, cuando corresponda, con el consentimiento libre, específico e informado del titular.

14. Seguridad de los datos personales

SECURITY DATA aplicara medidas de seguridad razonables y proporcionales al riesgo para proteger los datos personales frente a accesos no autorizados, alteración, pérdida, divulgación, uso indebido, incidentes, amenazas o vulnerabilidades.

En atención a la naturaleza de los servicios de certificación de información, firma electrónica y servicios relacionados, las medidas de seguridad se orientarán especialmente a proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Las medidas podrán incluir, según corresponda:

- Controles de acceso físico y lógico.
- Gestión de identidades, usuarios, roles y privilegios.
- Autenticación robusta y trazabilidad de accesos.
- Registro, monitoreo y auditoria de operaciones.
- Cifrado de información en tránsito y en reposo, cuando sea aplicable.
- Segmentación de sistemas y principio de menor privilegio.
- Respallos, recuperación y continuidad operativa.
- Gestión de vulnerabilidades, incidentes y eventos de seguridad.
- Protección de logs, evidencias, expedientes y registros electrónicos.
- Capacitación, confidencialidad y controles aplicables a trabajadores, proveedores, contratistas y terceros vinculados.
- Evaluación de riesgos y, cuando corresponda, evaluación de impacto en protección de datos personales.

15. Derechos de los titulares y procedimiento de atención

Los titulares podrán ejercer los derechos reconocidos por la normativa aplicable, incluyendo, según corresponda, derecho de información, acceso, rectificación y actualización, oposición, suspensión del tratamiento, portabilidad, derecho a no ser objeto de decisiones basadas únicamente en valoraciones automatizadas, retiro del consentimiento cuando el tratamiento se base en este, derecho a presentar reclamos ante la autoridad de control competente y demás derechos previstos en la LOPDP.

El titular podrá ejercer sus derechos mediante solicitud dirigida a SECURITY DATA a través de los siguientes canales:

- Correo electrónico: delegadodatos@securitydata.net.ec
- Formulario web: https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/Formulario_Derechos_Titulares_Dato_Personal.pdf
- Dirección física: cualquier sucursal de SECURITY DATA a nivel nacional.

SECURITY DATA atenderá las solicitudes, peticiones, quejas o reclamaciones relacionadas con el ejercicio de derechos de los titulares dentro del término de diez (10) días contados desde la recepción de la solicitud completa, sin perjuicio de los plazos especiales previstos en la normativa aplicable.

Cuando la solicitud sea incompleta, imprecisa, confusa o requiera aclaración, SECURITY DATA podrá requerir al titular, por una sola vez y dentro del término de cinco (5) días de recibida la solicitud, que aclare o complete la información necesaria para su atención. El titular contará con el término de diez (10) días, contados desde el día siguiente a la notificación del requerimiento, para completar o aclarar la solicitud.

Cuando la solicitud no pueda ser atendida en los términos requeridos por el titular debido a obligaciones legales, regulatorias, contractuales, de seguridad, trazabilidad, auditoria, control o defensa jurídica, SECURITY DATA emitirá una respuesta motivada dentro del término aplicable.

16. Cookies, tecnologías similares y canales digitales

SECURITY DATA podrá utilizar cookies, herramientas de analítica, tecnologías de seguimiento u otras tecnologías similares en su sitio web, plataformas, aplicaciones, formularios o canales digitales, con la finalidad de permitir su funcionamiento, mejorar la experiencia del usuario, medir el rendimiento de los servicios digitales, gestionar formularios, fortalecer la seguridad, prevenir fraude, atender requerimientos, generar métricas agregadas y cumplir obligaciones legales o regulatorias.

A través de estas tecnologías, SECURITY DATA podrá tratar datos técnicos derivados del uso de sus canales digitales, tales como dirección IP, identificadores de dispositivo, tipo de navegador, registros de navegación, fecha y hora de acceso, servicio consultado, formularios enviados, preferencias, logs, metadatos u otra información técnica necesaria para las finalidades antes indicadas.

Cuando el uso de cookies, analítica, tecnologías de seguimiento o herramientas de terceros requiera consentimiento o información específica, SECURITY DATA procurará implementar mecanismos informativos y de gestión que permitan al usuario conocer su uso, aceptar, rechazar o configurar dichas tecnologías, según corresponda conforme a la normativa aplicable.

En caso de que SECURITY DATA apruebe una Política de Cookies o documento específico sobre

tecnologías similares, dicha política complementara la Política de Privacidad y Tratamiento de Datos Personales y estará disponible en el sitio web institucional o en el canal que SECURITY DATA habilite para el efecto.

17. Video vigilancia

Cuando SECURITY DATA utilice sistemas de video vigilancia, el tratamiento de imágenes se realizará con fines de seguridad física, control de acceso, protección de personas, bienes, instalaciones e información.

Las zonas video vigiladas deberán contar con avisos informativos visibles. No se instalarán cámaras en lugares donde pueda afectarse injustificadamente la intimidad o privacidad de las personas, tales como baños, vestidores, lactarios, comedores u otros espacios de naturaleza privada o sensible.

SECURITY DATA no utilizara grabación de audio en sistemas de video vigilancia cuando ello implique captación de conversaciones privadas, control desproporcionado del desempeño laboral o afectación ilegítima de la intimidad, privacidad, libertad de expresión o protección de datos personales de trabajadores, visitantes, clientes, proveedores o terceros.

18. Redes sociales

Los canales de Instagram, X, Facebook, LinkedIn, YouTube u otros que utilice SECURITY DATA tienen un fin informativo, institucional y divulgativo. Dichos canales no constituyen medios formales para la presentación de solicitudes de ejercicio de derechos, denuncias, reclamaciones o consultas jurídicas en materia de protección de datos personales, las cuales deberán presentarse a través de los canales oficiales indicados en esta Política.

Los contenidos gráficos, de audio o video compartidos en los canales institucionales son de titularidad de SECURITY DATA o se publican conforme a las autorizaciones correspondientes y se encuentran protegidos por la normativa aplicable en materia de propiedad intelectual.

SECURITY DATA podrá moderar, modificar o retirar publicaciones, comentarios o mensajes en sus perfiles institucionales cuando resulten contrarios a la ley, a la finalidad del canal, a derechos de terceros, a la seguridad de la información o a las políticas institucionales aplicables.

19. Gestión de incidentes

SECURITY DATA contará con procedimientos internos para identificar, reportar, analizar, contener, mitigar, documentar y gestionar incidentes de seguridad que involucren datos personales.

Cuando una vulneración de seguridad pueda afectar derechos o libertades de los titulares, SECURITY DATA evaluará la procedencia de realizar las notificaciones correspondientes a la Autoridad de Protección de Datos Personales y/o a los titulares afectados, conforme a la normativa aplicable.

20. Actualización y vigencia

SECURITY DATA podrá actualizar esta Política cuando existan cambios normativos, regulatorios, tecnológicos, operativos, contractuales, institucionales o de riesgo que lo justifiquen.

La versión vigente de esta Política estará disponible en el sitio web institucional de SECURITY DATA o en el canal que la organización habilite para el efecto. Cuando los cambios sean sustanciales, SECURITY DATA podrá comunicarlos a los titulares por los medios que considere adecuados.

La presente Política rige a partir de su aprobación y permanecerá vigente mientras SECURITY DATA realice tratamiento de datos personales, sin perjuicio de sus modificaciones, actualizaciones o sustituciones posteriores.

Fecha de actualización: 29 de junio del 2026

