
 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	1




DECLARACIÓN DE
PRÁCTICAS DE
CERTIFICACIÓN DE
SELLADO DE
TIEMPO

febrero 13
2026

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	2


HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	FECHA	ELABORADO POR	REVISADO POR	APROBADO POR
1	EDICIÓN INICIAL	18/12/2025	SUPERVISOR LEGAL	CHIEF TECHNOLOGY OFFICER (CTO)	GERENTE GENERAL
2	<p>En el apartado 3.2.1., se adiciona el método para demostrar la posesión de la clave privada en caso de compra.</p> <p>Se modifica el apartado 4.1.2., se adiciona que la prestación del servicio estará sujeta a un contrato. Se coloca el tiempo de tramitación de solicitudes.</p> <p>Se adiciona el plazo de gracia para la solicitud de revocación.</p> <p>Se adiciona los requisitos de comprobación de revocación de CRL.</p> <p>Se modifica el apartado 5.5.2. y se adiciona como se garantiza la Seguridad Jurídica y el No Repudio a largo plazo.</p> <p>Se coloca de forma específica el procedimiento para compromiso confirmado o sospecha de la clave privada.</p> <p>Se adiciona la interoperabilidad del certificado.</p> <p>Se modifica todo el apartado 6.1.6..</p> <p>Se adiciona el apartado 6.2.7.</p> <p>Se modifica el apartado 6.8.3. y se adiciona la garantía de precisión de sincronización.</p> <p>Se enumeran todos los apartados.</p>	13/02/2026	SUPERVISOR LEGAL	CHIEF TECHNOLOGY OFFICER (CTO)	GERENTE GENERAL

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	3

Contenido


1.	Introducción.....	6
1.1.	Descripción general.	6
1.2.	Nombre e identificación del documento.....	6
1.3.	Participantes en los servicios de certificación.	6
1.3.1.	Autoridad de certificación (AC).	7
1.3.2.	Autoridades de registro (AR).	7
1.3.3.	Prestador de servicios de certificación.....	7
1.3.4.	Suscriptores.	7
1.3.5.	Terceros que confían.	7
1.4.	Usos del servicio de Sellado de Tiempo.....	7
1.4.1.	Usos apropiados.	7
1.4.2.	Usos prohibidos.....	8
1.5.	Administración de las Políticas.	8
1.5.1.	Organización que administra el documento.	8
1.5.2.	Persona de contacto.....	8
1.5.3.	Persona que determina la idoneidad de la política.....	9
1.5.4.	Procedimiento de Aprobación.....	9
1.6.	Definiciones y acrónimos.....	9
1.6.1.	Definiciones.	9
1.6.2.	Acrónimos.....	10
2.	Repositorios y Publicación de Información.	11
2.1.	REPOSITORIOS.	11
2.2.	PUBLICACIÓN DE INFORMACIÓN.....	11
2.2.1.	Políticas y Prácticas de Certificación.	11
2.3.	FRECUENCIA DE PUBLICACIÓN.	11
2.4.	CONTROL DE ACCESO A LOS REPOSITORIOS.	11
3.	Identificación y Autenticación.	11
3.1.	DENOMINACIÓN.	11
3.2.	VALIDACIÓN INICIAL DE LA IDENTIDAD.	12
3.3.	IDENTIFICACIÓN Y AUTENTICACIÓN EN LA RENOVACIÓN DE CERTIFICADOS.	14
3.4.	IDENTIFICACIÓN Y AUTENTICACIÓN EN LA REVOCACIÓN DE CERTIFICADOS.	14
4.	Requisitos Operaciones para el Ciclo de Vida de Los Certificados.	14
4.1.	Solicitud de Certificados.	14

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	4

4.2.	Procesos de Solicitud de Certificados.....	15
4.3.	Emisión del Sello de Tiempo.....	15
4.4.	Aceptación del certificado.....	16
4.5.	Uso de pares de claves y el certificado.....	16
4.6.	Renovación del Certificado.....	17
4.7.	Modificación de certificados.....	18
4.8.	Revocación y suspensión de certificados.....	18
4.9.	Servicio de información del estado de certificados.....	23
4.10.	Finalización de la Suscripción.....	23
4.11.	Custodia y recuperación de claves.....	24
5.	Gestión de instalaciones y controles operacionales.....	24
5.1.	Controles de seguridad física.....	24
5.2.	Controles de Procedimientos.....	26
5.3.	Control de personal.....	27
5.4.	Procedimientos de Registro de Auditoria.....	29
5.5.	Archivos de Registros.....	31
5.6.	Cambio de Claves de la TSA.....	32
5.7.	Recuperación ante Compromiso y Desastre.....	33
5.8.	Cese de Actividad.....	33
6.	Controles técnicos de seguridad.....	34
6.1.	Generación e Instalación del Par de Claves.....	34
6.2.	Protección de la Clave Privada y Controles de Ingeniería de los Módulos Criptográficos.....	36
6.3.	Otros Aspectos de la Gestión del Par de Claves.....	38
6.4.	Datos de Activación.....	38
6.5.	Controles de Seguridad Informática.....	39
6.6.	Controles de Seguridad del Ciclo de Vida.....	40
6.7.	Controles de Seguridad de la Red.....	42
6.8.	Sellado de Tiempo.....	42
7.	Perfiles del certificado TSA.....	43
7.1.	Perfil de los Certificados.....	43
7.2.	Perfil CRL.....	44
7.3.	PERFIL OCSP.....	45
8.	Auditorías de cumplimiento y otros controles.....	45

CÓDIGO	SD-ID-PE-14
VERSIÓN	V2
FECHA DE APROBACIÓN	13/02/2026
PÁGINAS	5

8.1.	FRECUENCIA DE LAS AUDITORIAS.....	45
8.2.	CUALIFICACIÓN DEL AUDITOR.....	45
8.3.	RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA	45
8.4.	ASPECTOS CUBIERTOS POR LOS CONTROLES	45
8.5.	ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE INCIDENCIAS.....	46
8.6.	COMUNICACIÓN DE RESULTADOS.....	46
9.	Otras cuestiones legales y de actividad.....	46
9.1.	TARIFAS.....	46
9.2.	Responsabilidades Financieras.....	47
9.3.	Confidencialidad de la Información.....	48
9.4.	Privacidad de la Información Personal.....	49
9.5.	Derechos de Propiedad Intelectual.....	50
9.6.	Declaraciones y Garantías.....	50
9.7.	Renuncias de Garantías.....	51
9.8.	Limitaciones de Responsabilidad.....	51
9.9.	Indemnizaciones.....	52
9.10.	Vigencia y Terminación.....	52
9.11.	notificación individuales y comunicación.....	52
9.12.	Enmiendas.....	52
9.13.	Procedimiento de resolución de disputas.....	53
9.14.	conformidad con la ley aplicable.....	53
9.15.	Cumplimiento de la Ley Aplicable.....	53
9.16.	Provisiones Misceláneas.....	53
9.17.	Otras Provisiones.....	54
10.	Control de aprobaciones.....	54

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	6

1. Introducción.

1.1. DESCRIPCIÓN GENERAL.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A, en lo sucesivo SECURITY DATA es una entidad certificadora que nació con el fin de cubrir las necesidades del mercado ecuatoriano de firma electrónica y certificados digitales.

SECURITY DATA es una empresa constituida de acuerdo a la legislación ecuatoriana, inscrita en el registro mercantil bajo el numero 2246 el 13 de Julio del 2010 con existencia legal hasta el 13 de Julio del 2060.

Los Servicios de Certificación de Información y Servicios Electrónicos Relacionados ofrecidos por SECURITY DATA están orientados a Personas particulares, Corporaciones Públicas y Privadas (como empresas, entidades públicas) y su objetivo es acreditar la identidad digital de las corporaciones y las personas naturales que actúan a través de la red.


Este documento declara las prácticas de certificación para el servicio de expedición de sellos de tiempo electrónicos de SECURITY DATA, mediante la explotación de la infraestructura de clave pública (PKI).

La estructura de este documento está basada en la especificación del estándar "RFC3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", creado por el grupo de trabajo PKIX del IETF. Adicionalmente a las Condiciones Generales establecidas en esta DPC, cada tipo de certificado emitido por SECURITY DATA se rige por unas condiciones particulares de emisión recogidas en un documento denominado "Política de Certificación" (en inglés CP o Certificate Policy).

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO.

Nombre:	Declaración de Prácticas de Certificación de Sellado de Tiempo (DPC)
Código del documento:	SD-ID-PE-14
Versión:	2
Descripción:	Declaración de Prácticas de Certificación de Sellado de Tiempo de Security Data Seguridad en Datos y Firma Digital S.A.
Fecha de emisión:	12 de febrero del 2026
Dirección:	Alonso de Torres y Av. Del Parque, Centro Comercial El Bosque oficinas administrativas C8
Número de teléfono:	023922169
Sitio Web:	www.securitydata.net.ec

1.3. PARTICIPANTES EN LOS SERVICIOS DE CERTIFICACIÓN.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	7

1.3.1. Autoridad de certificación (AC).

El sistema de certificación de Security Data Seguridad en Datos y Firma Digital está compuesto por diversas Autoridades de Certificación (en inglés CA o Certificate Authority) organizadas bajo una Jerarquía de Certificación.

1.3.2. Autoridades de registro (AR).

Security Data Seguridad en Datos y Firma Digital como autoridad de registro, es la responsable de realizar la verificación de identidad de los solicitantes de certificados digitales, así como de validar, aprobar o rechazar las solicitudes de emisión, renovación, revocación o suspensión de dichos certificados.

1.3.3. Prestador de servicios de certificación.

El Prestador de Servicios Electrónicos de Certificación (PSC) es la persona, física o jurídica, que presta uno o más servicios de certificación. Security Data es un PSC en cumplimiento con su Declaración de Prácticas de Certificación (DPC) que emite certificados reconocidos según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

1.3.4. Suscriptores.

Los suscriptores del servicio de certificación son los usuarios finales de los sellos de tiempo electrónicos expedidos por SECURITY DATA. Los suscriptores pueden ser personas naturales o jurídicas.

1.3.5. Terceros que confían.


Son las personas naturales o jurídicas que voluntariamente confían y hacen uso de los sellos de tiempo emitidos por SECURITY DATA.

Los sellos de tiempo emitidos por SECURITY DATA tienen carácter universal y están aceptados por los organismos públicos del estado ecuatoriano, como Ministerios, Secretarías, etc.

1.4. USOS DEL SERVICIO DE SELLADO DE TIEMPO.

1.4.1. Usos apropiados.

El servicio de sellado de tiempo proporcionado por SECURITY DATA como Autoridad de Sellado de Tiempo podrá ser utilizado exclusivamente para generar evidencias electrónicas confiables que acrediten la existencia de datos electrónicos en una fecha y hora determinadas, de conformidad con la normativa técnica aplicable y la legislación vigente en la República del Ecuador.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	8

El servicio de sellado de tiempo está destinado a respaldar la integridad y autenticidad de documentos electrónicos, mensajes de datos, transacciones digitales, registros informáticos y cualquier otro conjunto de información electrónica, conforme a lo establecido en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

1.4.2. Usos prohibidos.

El servicio de sellado de tiempo proporcionado por SECURITY DATA no podrá ser utilizado para fines distintos a los expresamente permitidos en la presente Declaración de Prácticas de Certificación ni en contravención a la normativa legal vigente en la República del Ecuador.

Los siguientes usos se consideran no autorizados:

- La utilización del servicio para fines ilícitos, fraudulentos o contrarios al ordenamiento jurídico ecuatoriano, incluyendo aquellos que vulneren la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su reglamento, la Ley Orgánica de Protección de Datos Personales y demás normas aplicables.
- La generación o intento de generación de sellos de tiempo con el objeto de crear, alterar, encubrir o validar evidencias electrónicas falsas, engañosas o manipuladas.
- El uso del servicio para respaldar contenidos, transacciones o actividades que vulneren derechos fundamentales, derechos de terceros o normas de orden público.
- El empleo del servicio con el fin de eludir controles legales, regulatorios, contractuales o judiciales, o para obstaculizar procesos de fiscalización, auditoría o investigación.
- El uso del servicio de sellado de tiempo en sistemas, aplicaciones o procesos no declarados o no compatibles con las políticas técnicas y de seguridad establecidas por la TSA.
- La solicitud de sellos de tiempo que impliquen un tratamiento de datos personales sin base legal, sin finalidad legítima o en incumplimiento de los principios establecidos en la Ley Orgánica de Protección de Datos Personales.


1.5. ADMINISTRACIÓN DE LAS POLÍTICAS.

1.5.1. Organización que administra el documento.

SECURITY DATA es responsable de la administración de esta DPC y de las Políticas de Certificación de Sellado de Tiempo.

1.5.2. Persona de contacto.

Nombre:	Lenin Alberto Vásquez Gonzalez
---------	--------------------------------

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	9

Dirección:	Alonso de Torres y Edmundo Carvajal Centro Comercial “El Bosque” Oficinas Administrativas piso 1.
Domicilio:	Quito - Ecuador
Correo electrónico:	cto@securitydata.net.ec
Teléfono:	(02) 3922169
Página web:	www.securitydata.net.ec

1.5.3. Persona que determina la idoneidad de la política.

La idoneidad de la presente política es determinada por el Supervisor Legal y el Chief Technology Officer (CTO) quienes son los encargados de evaluar y aprobar que su contenido sea adecuado, suficiente y coherente con los servicios prestados, los requisitos establecidos en la RFC 3647, así como con la normativa legal y regulatoria aplicable.

1.5.4. Procedimiento de Aprobación.

La publicación de las revisiones de esta DPC y de las PC de Sellado de Tiempo deberán ser aprobadas por la Alta Dirección de Security Data, después de comprobar el cumplimiento de los requisitos expresados en ellas.

1.6. DEFINICIONES Y ACRÓNIMOS.

1.6.1. Definiciones.


Certificado Electrónico: Es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Clave Pública y Clave Privada: La criptografía asimétrica en la que se basa la PKI emplea un par de claves (podrían ser dos pares de claves), lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

Firma Electrónica: Es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

Firma Electrónica Avanzada: Es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

Función Hash: Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo,

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	10

independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

Listas de Certificados Revocados (CRL): lista donde figuran las relaciones de certificados revocados o suspendidos.

Módulo Criptográfico Hardware (HSM): Módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.


Autoridad de Sellado de Tiempo (TSA): Entidad de confianza que emite sellos de tiempo.

Autoridad de Validación (VA): Entidad de confianza que proporciona información sobre la validez de los certificados digitales y de las firmas electrónicas.

Tercero Vinculado: Entidad de confianza que proporciona y/o administra los servicios de certificación.

1.6.2. Acrónimos.

AC:	Autoridad de Certificación
AC Sub:	Autoridad de Certificación Subordinada
PC:	Política de Certificación
DPC:	Declaración de Prácticas de Certificación
CRL:	Lista de Certificados Revocados (Certificate Revocation List)
HSM:	Módulo de seguridad criptográfico (Hardware Security Module)
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
PKI:	Infraestructura de Clave Pública (Public Key Infrastructure)
PSC:	Prestador de Servicios de Certificación
TSA:	Autoridad de sellado de tiempo (Time Stamp Authority)
VA:	Autoridad de validación (Validation Authority)
ECI:	Entidad de Certificación de Información
OID:	Identificador de objeto único (Object identifier)
DN:	Nombre Distintivo (Distinguished Name)
C:	País (Country)
CN:	Nombre Común (Common Name)
O:	Organización (Organization)
OU:	Unidad Organizacional (Organizational Unit)
SN:	Apellido (SurName)
ISO:	International Organization for Standardization
PKCS:	Public Key Cryptography Standards, Estándares PKI
UTF8:	Único de Transformation Format – 8 bits.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	11

TSU: Unidad de Sellado de Tiempo.

2. Repositorios y Publicación de Información.

2.1. REPOSITARIOS.

Los repositorios de Security Data están referenciados por la URL: https://www.securitydata.net.ec/ayuda-security-data-ecuador/#tabs_firma|3
Cualquier cambio en las URLs se notificará a todas las entidades que puedan verse afectadas.

Las direcciones IP correspondientes a cada URL podrán ser múltiples y dinámicas, pudiendo ser modificadas sin previo aviso.

2.2. PUBLICACIÓN DE INFORMACIÓN

2.2.1. Políticas y Prácticas de Certificación.

Tanto la DPC actual como las Políticas de Certificación de Sellado de Tiempo estarán disponibles en formato electrónico en la página web de Security Data.

Las versiones anteriores serán retiradas de su consulta on-line, pero podrán ser solicitadas por los interesados en la dirección de contacto de Security Data.

2.3. FRECUENCIA DE PUBLICACIÓN.

SECURITY DATA publicará de forma inmediata cualquier modificación en la Declaración de Prácticas y Políticas de certificación de Sellado de Tiempo.

2.4. CONTROL DE ACCESO A LOS REPOSITARIOS.


La presente DPC y las Políticas de Certificación de Sellado de Tiempo se publicarán en repositorios de acceso público sin control de acceso.

3. Identificación y Autenticación.

3.1. DENOMINACIÓN.

3.1.1. Tipos de nombres.

Los certificados electrónicos utilizados para la expedición del servicio de Sellado de Tiempo requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500. Adicionalmente, todos los nombres de los certificados reconocidos son coherentes con lo dispuesto en las normas:

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	12

- ETSI TS 101 862 conocida como "European profile for Qualified Certificates"
- RFC 5280 " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",
- RFC 3739 "Qualified Certificates Profile".
- RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"

3.1.2. Necesidad de que los nombres tengan significado.

Los campos del DN en los certificados electrónicos utilizados para la expedición del servicio de Sellado de Tiempo referentes a los datos correctos de la persona natural, persona Jurídica Pública o Privada que adquirió los servicios.

En el caso que los datos consignados en el DN fueran ficticios o se indique expresamente su invalidez (ej. "PRUEBA" o "INVALIDO"), se considerará al certificado sin validez legal, únicamente válido para realizar pruebas técnicas de interoperabilidad.

3.1.3. Anonimato o seudónimo de los suscriptores.

No es aplicable.

3.1.4. Reglas para la interpretación de las distintas formas de nombres.

Security Data atiende en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

3.1.5. Unicidad de los nombres.

El nombre distinguido (DN) de los certificados emitidos utilizados para la expedición del servicio de Sellado de Tiempo será único para cada persona Jurídica Pública o Privada. El atributo de CIF o NIF se usan para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.


3.1.6. Reconocimiento, autenticación y función de las marcas.

No es aplicable.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD.

Security Data no realiza la validación de la identidad de los suscriptores como requisito para la emisión del certificado o servicio de Sellado de Tiempo para personas naturales o jurídicas.

Cuando la solicitud es realizada por una persona jurídica, la validación inicial se limita a la verificación de la existencia legal de la persona jurídica solicitante, así como a la comprobación

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	13

de que la solicitud es realizada por su representante legal debidamente acreditado o por un miembro autorizado de la organización.

3.2.1. Método para demostrar la posesión de la clave privada.

No aplica la demostración de la posesión de clave privada por parte de usuarios o suscriptores, dado que el servicio de sellado de tiempo es prestado de forma automática por Security Data como TSA, siendo esta la única entidad que posee y controla las claves criptográficas utilizadas para la emisión de los sellos de tiempo.

En los casos en que el suscriptor solicite un certificado de Sello de Tiempo para ser operado de forma externa, la posesión de la clave privada se demostrará mediante la entrega de una solicitud de certificación firmada generada en un dispositivo seguro.

3.2.2. Autenticación de la identidad de la organización.

La autenticación de la identidad de una organización se limita a la verificación de la existencia legal de la persona jurídica solicitante, así como la comprobación de que la solicitud es realizada por su representante legal debidamente acreditado o por un miembro de empresa autorizado de la organización.

3.2.3. Autenticación de la identidad individual.

El servicio de sellado de tiempo no contempla la autenticación de identidad de personas naturales.

3.2.4. Información de suscriptor no verificada.


No es aplicable.

3.2.5. Validación de la autoridad.

Security Data valida su autoridad para la prestación del servicio de sellado de tiempo mediante la verificación de su existencia legal, capacidad jurídica y acreditación vigente, otorgada por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), conforme a lo establecido en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su normativa complementaria y las resoluciones técnicas emitidas por el ente regulador.

3.2.6. Criterios de interoperabilidad.

Los sellos de tiempo emitidos por Security Data se generan conforme a estándares técnicos internacionalmente reconocidos, garantizando su interoperabilidad y posibilidad de validación por parte de sistemas, aplicaciones y terceros que confían y disponen del certificado raíz y subordinado configurado

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	14

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN EN LA RENOVACIÓN DE CERTIFICADOS.

Security Data no realiza la validación de la identidad de los suscriptores como requisito para la renovación del certificado o servicio de Sellado de Tiempo para personas naturales o jurídicas.

Cuando la solicitud de renovación es realizada por una persona jurídica, la validación inicial se limita a la verificación de la existencia legal de la persona jurídica solicitante, así como a la comprobación de que la solicitud es realizada por su representante legal debidamente acreditado o por un miembro autorizado de la organización.

3.3.1. Identificación y autenticación para la renovación rutinaria de claves.

No es aplicable.

3.3.2. Identificación y autenticación para la renovación de claves después de la revocación.

No es aplicable.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN EN LA REVOCACIÓN DE CERTIFICADOS.

La identificación de los suscriptores en el proceso de revocación de certificados podrá ser realizada por:

- El envío del documento de identidad mediante correo electrónico.
- La presentación del documento de identidad del solicitante en las oficinas de Security Data.

4. Requisitos Operaciones para el Ciclo de Vida de Los Certificados.


4.1. SOLICITUD DE CERTIFICADOS.

4.1.1. Quién puede solicitar un Certificado.

El servicio de Sellado de Tiempo está disponible para personas naturales o jurídicas, públicas o privadas.

4.1.2. Proceso de inscripción y responsabilidades.

El solicitante deberá contactar a Security Data para gestionar la solicitud del servicio de Sellado de Tiempo, ya sea por medio del correo electrónico soporte@securitydata.net.ec o presencialmente en las oficinas de Security Data o de alguno de los Terceros Vinculados asociados.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	15

Si el solicitante requiere el servicio de sellado de tiempo para una organización deberá presentar la documentación necesaria para verificar la existencia legal de la persona jurídica, es decir:

- Documento de identidad del representante legal.
- Escritura o constitución.
- RUC
- Nombramiento del representante legal y su inscripción en el Registro Mercantil.
- Carta de autorización firmada por el representante legal en caso de miembros de empresa.

La prestación del servicio estará sujeta a la suscripción de un contrato de suscriptores de servicios aprobado por la autoridad competente o la aceptación de las condiciones generales de uso por parte del suscriptor

4.2. PROCESOS DE SOLICITUD DE CERTIFICADOS.

4.2.1. Realización de funciones de identificación y autenticación.

Es responsabilidad de Security Data, o del Tercero Vinculado debidamente autorizado, verificar de manera fehaciente la existencia legal de la persona jurídica solicitante, así como comprobar que la persona que actúa en su nombre cuenta con la calidad de representante legal, apoderado o miembro autorizado de la organización, conforme a la documentación habilitante correspondiente.

4.2.2. Aprobación o rechazo de solicitudes de certificados.

Una vez realizada la solicitud del certificado, el operador de registro de Security Data deberá verificar la información proporcionada por el solicitante.

Adicionalmente, también el Solicitante deberá aceptar las condiciones de uso y política de privacidad. Tras obtener las evidencias, se comprobará con las evidencias generadas por el sistema para aceptar o rechazar la validez de la solicitud.


Si la información no es correcta, se denegará la petición, comunicando al solicitante el motivo.

4.2.3. Tiempo de tramitación de las solicitudes de certificados.

El tiempo promedio para tramitar las solicitudes de los certificados de sellado de tiempo es de 24 a 48 horas laborables a partir de la validación completa de la documentación.

4.3. EMISIÓN DEL SELLO DE TIEMPO.

4.3.1. Acciones de la CA durante la emisión del certificado.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	16

Los certificados de sellado de tiempo se emitirán en el dispositivo criptográfico seguro (HSM) de Security Data.

Los sellos de tiempo son generados en respuesta a solicitudes válidas, conforme a los mecanismos técnicos y de seguridad establecidos, garantizando la integridad de la información sellada y la exactitud de la fecha y hora consignadas. La emisión del sello de tiempo se efectúa sin intervención manual, asegurando la continuidad, disponibilidad y consistencia del servicio.

Los certificados electrónicos utilizados para la emisión de los sellos de tiempo forman parte integral del servicio y se emplean exclusivamente para la generación, firma y verificación de los sellos de tiempo, de acuerdo con las políticas y prácticas definidas en la presente Declaración de Prácticas de Certificación.

4.3.2. Notificación al suscriptor por parte de la CA de la emisión del certificado.

Una vez el certificado de sellado de tiempo haya sido emitido, el solicitante recibirá de parte del Security Data un correo con la URL, el usuario, contraseña y el número de sellos disponibles.

4.4. ACEPTACIÓN DEL CERTIFICADO.

4.4.1. Conducta que constituye la aceptación del certificado.

El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el suscriptor y Security Data haya sido firmado. En consecuencia, la aceptación del servicio de sellado de tiempo se entenderá realizada cuando el suscriptor haga uso efectivo del certificado para la generación de un sello de tiempo en el firmado de un documento electrónico.

4.4.2. Publicación del certificado por la CA.

No es aplicable.

4.4.3. Notificación de la emisión de certificados por parte de la CA a otras entidades.


No es aplicable.

4.5. USO DE PARES DE CLAVES Y EL CERTIFICADO.

4.5.1. Uso de la clave privada y del certificado del suscriptor.

La clave privada asociada al certificado utilizado para la prestación del servicio de sellado de tiempo es de uso exclusivo de Security Data y se emplea únicamente para la generación y firma de sellos de tiempo, conforme a los procedimientos establecidos en la presente DPC.

4.5.2. Uso de clave pública y certificado de la parte que confía.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	17

Las partes que confían utilizan la clave pública contenida en el certificado únicamente para verificar la autenticidad, integridad y validez de los sellos de tiempo emitidos, siendo los responsables de comprobar la vigencia y estado del certificado.

4.6. RENOVIACIÓN DEL CERTIFICADO.

4.6.1. Circunstancias para la renovación del certificado.

Los certificados electrónicos utilizados en la prestación del servicio de Sellado de Tiempo se renovarán próximo a la fecha de expiración del certificado.

4.6.2. Quién puede solicitar la renovación.

La renovación del servicio de Sellado de Tiempo lo puede realizar cualquier persona natural o jurídica, pública o privada.

4.6.3. Tramitación de solicitudes de renovación de certificados.

Security Data recibirá solicitudes de renovación de los certificados electrónicos utilizados en la prestación del servicio de Sellado de Tiempo mediante correo electrónico sopORTE@SECURITYDATA.NET.EC o presencialmente en las oficinas de Security Data o de alguno de los Terceros Vinculados asociados.

4.6.4. Notificación de la emisión de un nuevo certificado al suscriptor.

Una vez el certificado de sellado de tiempo haya sido renovado, el solicitante recibirá de parte del Security Data un correo con la URL, el usuario, contraseña y el número de sellos disponibles.

4.6.5. Conducta que constituye aceptación de un certificado de renovación.


El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el suscriptor y Security Data haya sido firmado. En consecuencia, la aceptación del servicio de sellado de tiempo se entenderá realizada cuando el suscriptor haga uso efectivo del certificado para la generación de un sello de tiempo en el firmado de un documento electrónico.

4.6.6. Publicación del certificado de renovación por parte de la CA.

La publicación del certificado de sello de tiempo se lo realizará según lo especificado en la normativa, mediante consulta del serial web.

4.6.7. Notificación de la emisión de certificados por parte de la CA a otras entidades.

No es aplicable.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	18

4.7. MODIFICACIÓN DE CERTIFICADOS.

4.7.1. Circunstancias para la modificación del certificado.

En caso de existir algún dato erróneo en el certificado electrónico utilizado en la prestación del servicio de Sellado de Tiempo, se deberá proceder a la revocación y a la emisión de un nuevo certificado con los datos modificados.

4.7.2. Quién puede solicitar la modificación del certificado.

La modificación del certificado usado para el servicio de Sellado de Tiempo lo debe realizar el titular del certificado.

4.7.3. Procesamiento de solicitudes de modificación de certificados.

Security Data recibirá solicitudes de modificación de los certificados electrónicos utilizados en la prestación del servicio de Sellado de Tiempo mediante correo electrónico soporte@securitydata.net.ec o presencialmente en las oficinas de Security Data o de alguno de los Terceros Vinculados asociados.

4.7.4. Notificación de la emisión de un nuevo certificado al suscriptor.

Una vez el certificado de sellado de tiempo haya sido emitido, el solicitante recibirá de parte de Security Data un correo con la URL, el usuario, contraseña y el número de sellos disponibles.

4.7.5. Conducta que constituye aceptación del certificado modificado.

El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el suscriptor y Security Data haya sido firmado. En consecuencia, la aceptación del servicio de sellado de tiempo se entenderá realizada cuando el suscriptor haga uso efectivo del certificado para la generación de un sello de tiempo en el firmado de un documento electrónico.


4.7.6. Publicación del certificado modificado por la CA.

La publicación del certificado de sello de tiempo se lo realizará según lo especificado en la normativa, mediante consulta del serial web.

4.7.7. Notificación de la emisión de certificados por parte de la CA a otras entidades.

No es aplicable.

4.8. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	19

La revocación de un certificado electrónico utilizado en la prestación del servicio de Sellado de Tiempo supone la pérdida de validez de este, y es irreversible. La suspensión no será aplicable para este tipo de certificados.

Las revocaciones tienen efecto desde el momento en que aparecen publicadas en la CRL.

4.8.1. Circunstancias de revocación.


Un certificado electrónico utilizado en la prestación del servicio de Sellado de Tiempo podrá ser revocado debido a las siguientes causas:

- a) Circunstancias que afectan a la información contenida en el certificado:
 - Modificación de alguno de los datos contenidos en el certificado.
 - Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
 - Pérdida o cambio de la vinculación del firmante con la Corporación.

- b) Circunstancias que afectan a la seguridad de la clave privada o del certificado:
 - Compromiso de la clave privada o de la infraestructura o sistemas de la TSA, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
 - Infracción, por parte de la TSA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la DPC.
 - Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor.
 - Acceso o utilización no autorizados, por un tercero, de la clave privada del suscriptor.
 - El uso irregular del certificado por el suscriptor o firmante.
 - El incumplimiento por parte del suscriptor o firmante de las normas de uso del certificado expuestas en la DPC o en el instrumento jurídico vinculante entre Security Data y el suscriptor.

- c) Circunstancias que afectan a la seguridad del dispositivo criptográfico:
 - Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
 - Pérdida o inutilización por daños del dispositivo criptográfico.
 - Acceso no autorizado, por un tercero, a los datos de activación del suscriptor.
 - El incumplimiento por parte del suscriptor o firmante de las normas de uso del certificado expuestas en la DPC o en el instrumento jurídico vinculante entre Security Data y el suscriptor.

- d) Circunstancias que afectan al suscriptor:
 - Finalización de la relación jurídica entre Security Data y el Suscriptor.
 - Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al firmante.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	20

- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
 - Infracción por el suscriptor, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en la DPC.
- e) Otras circunstancias:
- La suspensión del certificado digital por un período superior al establecido en la DPC.
 - Por resolución judicial o administrativa que lo ordene.
 - Por la concurrencia de cualquier otra causa especificada en la DPC.

4.8.2. Quién puede Solicitar la Revocación.

Pueden solicitar la revocación de un certificado electrónico utilizado en la prestación del servicio de Sellado de Tiempo:

- El propio suscriptor, que deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.
- Cualquier persona podrá solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

Podrán tramitar la revocación del certificado:

- Los operadores autorizados del Tercero Vinculado a la que pertenece el suscriptor del certificado.
- Los operadores autorizados de la TSA.

4.8.3. Procedimientos para la Solicitud de Revocación.

Existen distintas alternativas para el suscriptor a la hora de solicitar la revocación del certificado electrónico utilizado en la prestación del servicio de Sellado de Tiempo.


En todo caso, al tiempo de suspenderse o revocarse el certificado, se enviará un comunicado al suscriptor.

4.8.4. Plazo de gracia para la solicitud de revocación.

Se establece un plazo de gracia máximo de 24 horas para que el suscriptor notifique un compromiso de clave. Una vez verificada la identidad del solicitante, la revocación se procesará de manera inmediata

4.8.5. Revocación en Horario de Oficina.

El suscriptor o el firmante deberá ponerse en contacto con Security Data o el Tercero Vinculado asociado ya sea vía correo electrónico o personalmente.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	21

Si el suscriptor o firmante asiste personalmente, su identidad quedará autenticado mediante la presentación de su cédula de identidad o pasaporte. En caso de proceder con la revocación del certificado, esta se llevará a cabo de manera inmediata, una vez completada y firmada la solicitud de revocación y entregada al operador de Security Data.

Si lo hace vía correo electrónico a soporte@securitydata.net.ec, la solicitud de revocación deberá estar firmada electrónicamente y se procederá con la revocación definitiva.

Las revocaciones tienen efecto desde el momento en que aparecen publicadas en las CRL.

4.8.6. Revocación Fuera de Horario de Oficina.

El cliente solicitará la revocación por correo electrónico a soporte@securitydata.net.ec, la misma será procesada el siguiente día hábil a partir de las 8h00.

4.8.7. Plazo en el que la CA debe tramitar la Solicitud de Revocación.

Una vez la identidad del suscriptor haya sido autenticada según lo expuesto anteriormente, y la revocación debidamente tramitada por Security Data, la revocación se hará efectiva inmediatamente.

4.8.8. Requisito de comprobación de revocación para las partes que confían.

La verificación del estado de los certificados electrónicos utilizados en la prestación del servicio de Sellado de Tiempo es obligatoria, ya sea mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.

4.8.9. Frecuencia de Emisión de CRLs.

La CRL de los certificados de entidad final se emiten cada 24 horas o cuando se produzca una revocación y para una consulta rápida la entidad de certificación emite una CRL delta cada 4 horas.


La CRL de los certificados de autoridad (ARL) se emite cada 6 meses o cuando se produzca una revocación.

4.8.10. Latencia máxima para CRL.

Dado que la publicación de las CRL se realiza en el momento de la generación de esta, se considera cero o nulo el tiempo transcurrido.

4.8.11. Disponibilidad de comprobación de estado/revocación en línea.

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	22

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de Security Data, ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

4.8.12. Requisitos de comprobación de revocación en línea.

No es aplicable.

4.8.13. Requisitos de Comprobación de Revocación de CRL

Para el uso del servicio de CRLs, que es de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión "CRL Distribution Point".
- El usuario deberá comprobar adicionalmente la(s) CRL(s) pertinentes de la cadena de certificación de la jerarquía.
- El usuario deberá asegurarse que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.
- Los certificados revocados que expiren serán retirados de la CRL.

4.8.14. Otras formas de anuncios de revocación disponibles.

No es aplicable.


4.8.15. Requisitos especiales en materia de compromiso de claves.

- Compromiso de la clave privada o de la infraestructura o sistemas de la AC, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
- Infracción por parte de la AC o del Tercero Vinculado de los requisitos previstos en los procedimientos de gestión de certificados establecidos en la presente DPC.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor.
- Acceso o utilización no autorizadas por un tercero, de la clave privada del suscriptor.
- El uso irregular del certificado por el suscriptor o firmante.
- El incumplimiento por parte del suscriptor o firmante de las normas de uso del certificado expuestas en la presente DPC o en el instrumento jurídico vinculante entre Security Data Seguridad en Datos y Firma Digital y el suscriptor.

4.8.16. Circunstancias de suspensión.

No es aplicable.

4.8.17. Quién puede solicitar la suspensión.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	23

No es aplicable.

4.8.18. Procedimiento para solicitud de suspensión.

No es aplicable.

4.8.19. Límites del período de suspensión.

No es aplicable.

4.9. SERVICIO DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS.

4.9.1. Características operativas.

Security Data ofrece un servicio gratuito de publicación en la página web de las Listas de Certificados Revocados (CRL) sin restricciones de acceso las cuales contienen la lista de revocaciones desde su creación y son firmadas por la CA Raíz.

4.9.2. Disponibilidad del servicio.

Los enlaces de descarga los pueden encontrar en las siguientes direcciones:

CRLS SUBCA-2:

<http://crl1.securitydata.net.ec/subca2crl1/crlfile.crl>

<http://crl2.securitydata.net.ec/subca2crl2/crlfile.crl>

Security Data tiene todas las listas de revocación publicadas.

Adicionalmente, Security Data ofrece el servicio de validación de certificados mediante el protocolo OCSP (Online Certificate Status Protocol). La información al respecto se encuentra en la DCP de OSCP publicado en el siguiente enlace:


https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/Ocsp_DPC.pdf

4.9.3. Características opcionales.

No es aplicable.

4.10. FINALIZACIÓN DE LA SUSCRIPCIÓN.

La suscripción finalizará en el momento de expiración o revocación del certificado electrónico utilizado en la prestación del servicio de Sellado de Tiempo.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	24

4.11. CUSTODIA Y RECUPERACIÓN DE CLAVES.

4.11.1. Política y prácticas de depósito y recuperación de claves.

No es aplicable.

4.11.2. Política y prácticas de encapsulación y recuperación de claves de sesión.

No es aplicable.

5. Gestión de instalaciones y controles operacionales.

5.1. CONTROLES DE SEGURIDAD FÍSICA.

Security Data tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios electrónicos de certificación ofrece protección frente:


- Accesos físico no autorizados
- Desastres naturales
- Incendios
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura
- Inundaciones
- Robo
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios de la Entidad Acreditada

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso. La localización de las instalaciones garantiza la presencia de fuerzas de seguridad en un plazo no superior a 30 minutos.

5.1.1. Ubicación Física y Construcción.

Las instalaciones de Security Data están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta, y ubicadas en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas es una jaula con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas anti-humedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	25

5.1.2. Acceso Físico.

El acceso físico a las dependencias de Security Data donde se llevan a cabo procesos de certificación de sellado de tiempo está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables, así como Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación y huella dactilar, gestionado por un sistema informático que mantiene un log de entradas y salidas automático.

5.1.3. Alimentación Eléctrica y Aire Acondicionado.

Las instalaciones de Security Data disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado mediante un grupo electrógeno redundante con depósitos de combustible que pueden ser rellenados desde el exterior.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4. Exposición al Agua.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.


5.1.5. Protección y Prevención contra Incendios.

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

5.1.6. Sistema de Almacenamiento.

Cada medio de almacenamiento desmontable (cintas, cartuchos, disquetes, etc.), que contenga información clasificada, está etiquetado con el nivel más alto de clasificación de la información que contenga y permanece solamente al alcance de personal autorizado.

La información con clasificación Confidencial, independientemente del dispositivo de almacenamiento, se guarda en armarios ignífugos o bajo llave permanentemente, requiriéndose autorización expresa para su retirada.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	26

5.1.7. Eliminación de los Soportes de Información.

Cuando haya dejado de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga:

- Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.
- Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado físicamente destruidos o hacer ilegible la información contenida.

5.1.8. Copia de Seguridad de la información

Se establecen respaldos diarios de la información.

5.2. CONTROLES DE PROCEDIMIENTOS.

5.2.1. Roles de los responsables.


Los roles de confianza son los que se describen en las respectivas Políticas de Certificación de la jerarquía de forma que se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación. Los roles mínimos establecidos son:

- Responsable de seguridad (Security Officer): Mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad.
- Administradores del sistema de certificación (System Administrators): Autorizado para realizar cambios en la configuración del sistema, pero sin acceso a los datos del mismo.
- Operadores de sistemas (System Operator): Responsables de la gestión del día a día del sistema (Monitorización, backup, recovery,...)
- Auditor interno (System Auditor): Autorizado a acceder a los logs del sistema y verificar los procedimientos que se realizan sobre el mismo.
- Operador de TSA - Operador de Certificación: Responsables de activar las claves de la TSA en el entorno Online, o de los procesos de firma de certificados y CRL's en el entorno Root Offline.
- Operador de Tercero Vinculado (Registration Officer): Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final.

5.2.2. Número de Personas Requeridas por Tarea.

Security Data garantiza al menos dos personas para realizar las tareas que requieren control multipersona y que se detallan a continuación:

- La generación de la clave de las TSA.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	27

- La recuperación y back-up de la clave privada de las TSA.
- La emisión de certificados de las TSA.
- Activación de la clave privada de las TSA.
- Cualquier actividad realizada sobre los recursos hardware y software que dan soporte a la root TSA.

5.2.3. Identificación y Autenticación por Rol.

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona sólo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales, tarjetas de acceso físico y llaves.

5.2.4. Roles que Requieren Segregación de Funciones.

Las tareas de Auditor son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría o Certificación.

5.3. CONTROL DE PERSONAL.


5.3.1. Requisitos Relativos a la Calificación, Conocimiento y Experiencia Profesionales.

Todo el personal que realiza tareas calificadas como confiables sin supervisión lleva al menos seis meses trabajando en el centro de producción y tiene contrato laboral fijo.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

Security Data se asegura que el personal de registro es personal confiable de la Corporación para realizar las tareas de registro. A tal efecto se exige una declaración en tal sentido por parte de la Entidad que asume funciones del Tercero Vinculado.

El operador del registro habrá realizado un curso de preparación para la realización de las tareas de registro y validación de las peticiones. Al final de dicho curso, se procederá a evaluar sus conocimientos del proceso.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	28

Security Data retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

5.3.2. Procedimientos de Comprobación de Antecedentes.

Security Data realiza las investigaciones pertinentes antes de la contratación de cualquier persona.

Los Terceros Vinculados pueden establecer criterios diferentes, siendo responsables por la actuación de las personas que autoricen.

5.3.3. Requerimientos de Formación.

Security Data realiza los cursos necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada operador.

5.3.4. Requerimientos y Frecuencia de Actualización de la Formación.

Security Data realizará capacitaciones continuas a todo el personal, al menos una vez al año en seguridad de la información.

5.3.5. Frecuencia y secuencia de rotación de puestos.

No aplica.

5.3.6. Requisitos del contratista independiente.


Los empleados contratados para realizar tareas confiables deberán firmar anteriormente las cláusulas de confidencialidad y los requerimientos operacionales empleados por Security Data.

Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

5.3.7. Sanciones por acciones no autorizadas.

Security Data emprenderá medidas disciplinarias cuando compruebe que se realizó alguna acción no autorizada.

Tras la detección de una acción no autorizada, Security Data dará inicio a un proceso de investigación para determinar la veracidad e impacto de la acción y los colaboradores involucrados. Posterior a esto se tomarán las medidas disciplinarias según la gravedad e intención de la acción.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	29

5.3.8. Requerimientos para contratación de personal.

Los requerimientos para contratación de personal nuevo en Security Data se verifican en el perfil y descriptivo de cada cargo. Entre estos requisitos principalmente constan la formación académica, experiencia y conocimientos necesarios para el cargo.

Adicionalmente el personal nuevo debe someterse a una valoración médica para comprobar que este Apto para el desempeño de sus funciones.

5.3.9. Documentación suministrada al personal.

A todo el personal incorporado dentro de Security Data se le proporciona la siguiente documentación:

- Reglamento Interno de Seguridad y Salud del Trabajo
- Reglamento Interno

5.4. PROCEDIMIENTOS DE REGISTRO DE AUDITORIA.

5.4.1. Tipos de eventos registrados.

Security Data registra y guarda los logs de todos los eventos relativos al sistema de seguridad de la TSA. Estos incluyen los siguientes eventos:


- Encendido y apagado del sistema.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la TSA a través de la red.
- Intentos de accesos no autorizados a la red interna.
- Intentos de accesos no autorizados al sistema de archivos.
- Cambios en la configuración y mantenimiento del sistema.
- Encendido y apagado de la aplicación de la TSA.

Adicionalmente, Security Data conserva, ya sea manual o electrónicamente, la siguiente información:

- Registros de acceso físico.
- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal que realiza tareas de confianza.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de suscriptor, si se gestiona esa información.

5.4.2. Frecuencia de Procesado de Registros de Auditoría.

Se revisarán los logs de auditoría cada semana y en todo caso cuando se produzca una alerta del

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	30

sistema motivada por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

5.4.3. Periodo de Conservación de los Registros de Auditoría.

Security Data almacenará la información de los logs de auditoría el tiempo que se considere necesario para garantizar las seguridades del sistema en función de la importancia de cada log en concreto.

5.4.4. Protección de los Registros de Auditoría.

Los logs de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen.

Son almacenados en dispositivos ignífugos. Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la Autoridad de Certificación.

Los dispositivos son manejados en todo momento por personal autorizado.

5.4.5. Procedimientos de Respaldo de los Registros de Auditoría.

Security Data dispone de un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

Security Data tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. El medio externo se almacena en armario ignífugo bajo medidas de seguridad que garantizan que su acceso solo está permitido a personal autorizado. Se realizan copias diarias incrementales y completas semanales.


Adicionalmente se mantiene copia de los logs de auditoría en centro de custodia externo.

5.4.6. Sistema de Recolección de Información de Auditoría.

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de certificación.

5.4.7. Notificación al sujeto causante del evento.

En caso de un evento crítico que afecte la validez o seguridad del servicio de sellado de tiempo, Security Data notificará formalmente al sujeto causante, detallando la naturaleza del evento y las acciones correctivas necesarias en caso que amerite. La notificación será formal y documentada, asegurando que las medidas correctivas se tomen dentro de un plazo razonable.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	31

5.4.8. Análisis de Vulnerabilidades.

Security Data realiza una revisión anual de discrepancias en la información de los logs y actividades sospechosas.

5.5. ARCHIVOS DE REGISTROS.

5.5.1. Tipo de Eventos Archivados.

Se conservarán los eventos que tengan lugar durante el ciclo de vida del certificado de sellado de tiempo, incluyendo la renovación del mismo. Se almacenará por Security Data o, por delegación de ésta en el Tercero Vinculado:

- Todos los datos de la auditoría
- Solicitudes de emisión y revocación de certificados
- Todos los certificados emitidos o publicados
- CRL's emitidas o registros del estado de los certificados generados
- La documentación requerida por los auditores
- Las comunicaciones entre los elementos de la PKI

Security Data es responsable del correcto archivo de todo este material y documentación.

5.5.2. Periodo de Conservación de Registros.


Todos los datos del sistema relativos al ciclo de vida de los certificados se conservarán durante el periodo que establezca la legislación vigente cuando sea aplicable. Los certificados se conservarán publicados en el repositorio durante al menos un año desde su expiración.

Los contratos con los suscriptores y cualquier información relativa a la identificación y autenticación del suscriptor serán conservados durante al menos 15 años o el periodo que establezca la legislación vigente.

Con el fin de garantizar la Seguridad Jurídica y el No Repudio a largo plazo, Security Data mantendrá disponibles las listas de revocación (CRL) históricas y los registros de auditoría incluso tras la expiración del certificado de la TSA. Esto permite que los terceros que confían puedan realizar la Validación a Largo Plazo (LTV) de los documentos sellados durante el periodo de vigencia del certificado, asegurando que la prueba de existencia sea válida ante procesos administrativos o judiciales futuros.

5.5.3. Protección del Archivo.

Security Data asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas en los casos en que así se requiera.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	32

Security Data dispone de documentos técnicos y de configuración donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

5.5.4. Procedimientos de Copia de Seguridad del Archivo.

Security Data dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

5.5.5. Requerimientos para el Sellado de Tiempo de los Registros.

Los registros están fechados con una fuente fiable.

Los procesos de generación de sellos de tiempo, se rigen y cumplen estrictamente con lo dispuesto en la Normativa Técnica Ecuatoriana en su Capítulo VI, artículo 22, literal D.

5.5.6. Sistema de Archivo de Información de Auditoría.

No estipulado.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Durante la auditoria requerida, el auditor verificará la integridad de la información archivada. El acceso a la información archivada se realiza solo por personal autorizado.

Security Data proporcionará la información y los medios al auditor para poder verificar la información archivada.

5.6. CAMBIO DE CLAVES DE LA TSA.


Antes de que el certificado de Security Data expire se realizará un cambio de claves (rekeying) y, en su caso, se introducirán cambios en el contenido del certificado de TSU que se ajusten mejor a la legislación vigente y la realidad de Security Data Seguridad en Datos y Firma Digital y del mercado. Se generará una nueva TSA con una clave privada nueva.

5.6.1. Procedimiento de actuación ante la vulnerabilidad de la clave privada de una TSA.

Se considera el compromiso o sospecha de su clave privada como un incidente y será atendido como un incidente mayor de la prestación de los servicios de certificación digital.

En caso de compromiso confirmado o sospecha fundada de la clave privada de la TSA, Security Data ejecutará un plan de comunicación de crisis que incluye:

1. Notificación inmediata al ente regulador;

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	33

2. Publicación de un aviso de alerta en la página web principal en un plazo máximo de una (1) hora; y,
3. Envío de notificaciones electrónicas a los suscriptores activos. El aviso indicará la fecha y hora exacta del compromiso para que los usuarios puedan identificar los sellos de tiempo que han perdido su presunción de integridad

5.7. RECUPERACIÓN ANTE COMPROMISO Y DESASTRE.

5.7.1. Procedimientos de Gestión de Incidentes y Vulnerabilidades.

Security Data en base a su infraestructura, puede recuperar todos los sistemas en menos de 48 horas, aunque se asegura la revocación y publicación de información del estado de los certificados en menos de 24 horas.

5.7.2. Alteración de los Recursos Hardware, Software y/o Datos.

En el caso de que tuviera lugar un incidente que alterará o corrompiera tanto recursos de hardware, software como datos, Security Data procederá según lo estipulado en el documento "Política de seguridad".

5.7.3. Procedimiento de Actuación ante la Vulnerabilidad de la Clave Privada de una Autoridad de Certificación.

En caso de compromiso de la clave privada de Security Data:


- Informará a todos los suscriptores, usuarios y otras TSA con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web de Security Data.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

5.7.4. Continuidad del Negocio después de un desastre.

- Security Data restablecerá los servicios críticos (Revocación y publicación de certificados revocados) de acuerdo con esta DPC dentro de las 24 horas posteriores a un desastre o emergencia imprevista.
- Se dispone de un centro alternativo, en caso de ser necesario, para la puesta en funcionamiento de los sistemas de certificación.
- La restauración se realiza de manera lógica.
- Los respaldos se ejecutan de manera diaria a nivel lógico con una retención de 7 días.

5.8. CESE DE ACTIVIDAD.

5.8.1. Autoridad de Certificación

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	34

Antes del cese de su actividad la TSA realizará las siguientes actuaciones:

- Proveerá de los fondos necesarios para continuar la finalización de las actividades de revocación hasta el cese definitivo de la actividad, si es el caso.
- Informará a todos los suscriptores, solicitantes, usuarios, otras TSA's o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.
- Revocará toda autorización a entidades subcontratadas que usen el TSA.
- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los certificados, especificando, en su caso, si se va a transferir la gestión y a quien.
- Los registros de la TSA se archivarán y se transferirán a un custodio específico.

6. Controles técnicos de seguridad.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.

6.1.1. Generación del Par de Claves.

Se distinguirán dos casos en la generación de claves para certificados reconocidos:

- a) En hardware HSM (soporte físico)


Accesos

El acceso al servicio de la Autoridad de Sellado de Tiempo (TSA) se realiza de conformidad con el proceso documentado de ceremonia de claves, dentro de la sala de seguridad de la Entidad Acreditada, utilizando dispositivos criptográficos de hardware (HSM). Dicho acceso es otorgado únicamente a personal debidamente autorizado, conforme a los roles de confianza definidos, bajo un esquema de control dual, y con la participación de testigos de SECURITY DATA, de la organización titular de la TSA y del auditor externo, garantizando que ninguna persona pueda acceder o realizar operaciones críticas de manera individual.

Generación del certificado

Las Entidades de Certificación de Información y Servicios Relacionados Acreditadas o Terceros Vinculados, deberán emitir los certificados de sellado de tiempo en dispositivos criptográficos seguros HSM (Módulos de Seguridad de Hardware) diseñados para proporcionar un entorno seguro y confiable para operaciones criptográficas, protegiendo de manera segura contra accesos no autorizados, definidos en el estándar RFC 3161, asegurando la interoperabilidad y la uniformidad en la implementación del sellado de tiempo en diferentes sistemas y aplicaciones.

- b) Servicio TSA

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	35

El suscriptor recibirá las credenciales de acceso al servicio de sellado de tiempo de SECURITY DATA, consistentes en una URL de acceso, usuario y contraseña, a través de un canal seguro previamente definido.

El acceso al servicio permitirá al suscriptor utilizar el número de sellos de tiempo contratados, dentro del período de vigencia establecido, sin que el suscriptor participe en la generación o custodia de claves criptográficas, las cuales son administradas exclusivamente por la Autoridad de Sellado de Tiempo (TSA) en su infraestructura segura.

El servicio de sellado de tiempo de Security Data es plenamente interoperable y cumple con los estándares internacionales y es compatible con perfiles avanzados de firma electrónica. Esto garantiza que los sellos de tiempo generados sean reconocidos por aplicaciones de terceros, lectores de PDF estándar y plataformas de administración pública

6.1.2. Entrega de la Clave Privada al Suscriptor.

- a) En hardware (soporte físico)

La clave privada será entregada junto al certificado en el dispositivo de creación de firma. El Tercero Vinculado será responsable de garantizar la entrega del dispositivo al suscriptor, asegurándose así que éste último está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

6.1.3. Entrega de clave pública al emisor del certificado.

El envío de la clave pública a la AC para la generación del certificado se realiza mediante un formato estándar preferiblemente en formato PKCS#10 o X.509 autofirmado, utilizando un canal seguro para la transmisión.

6.1.4. Entrega de la Clave Pública a los Terceros que Confían en los Certificados.

El certificado de las TSA de la cadena de certificación y su fingerprint (huella digital) estarán a disposición de los usuarios en la página web de Security Data Seguridad en Datos y Firma Digital.


6.1.5. Tamaño de Clave

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.6. Generación de parámetros de clave pública y control de calidad.

Generación

La generación del par de claves se realiza dentro del HSM asociado, mediante interfaz PKCS#11,.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	36

La operación de generación se ejecuta bajo doble control (Administrador del Sistema + Operador del Sistema) y queda registrada en:

- Bitácora del HSM (cuando aplique),
- Auditoría/logs de EJBCA,

Control de calidad

Para el control de calidad se verifican como mínimo:

- Verificación de tamaño y parámetros
- Longitud de módulo RSA ≥ 2048 bits
- Confirmación de que la clave fue creada correctamente.
- Validación criptográfica del par (p. ej. prueba de firma y verificación con la clave recién generada, o validación equivalente provista por el HSM).
- Verificación de estado saludable del HSM (self-tests/estado operacional)
- Registro de versión/firmware del HSM

6.1.7. Usos Admitidos de la Clave (campo KeyUsage de X.509v3).

Todos los certificados TSA incluyen la extensión Key Usage y Extended Key Usage, indicando los usos habilitados de las claves.

Se usa Firma Digital bajo el OID 2.5.29.15.

6.1.8. Extended Key Usage (EKU).

El EKU que se incluyen en los Certificados de TSA de Security Data S.A. es:

Timestamping 1.3.6.1.5.5.7.3.8


6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS.

6.2.1. Estándares para los Módulos Criptográficos.

Los módulos criptográficos empleados para generar y almacenar las claves de las Autoridades de Certificación están certificados con la norma FIPS-140-2 nivel 3.

Las claves de los suscriptores de certificados reconocidos con DSCF y de operadores y administradores son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico CC EAL4+, FIPS 140-1 nivel 3, ITSEC E4 High u otro de nivel equivalente.

Los dispositivos criptográficos de custodia de la clave privada del suscriptor de certificados reconocidos con DSCF y del operador o administrador aportan un nivel de seguridad.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	37

6.2.2. Control Multipersona (k de n) de la Clave Privada.

El acceso a las claves privadas de Security Data requiere el concurso simultáneo de tres dispositivos criptográficos diferentes de cinco posibles, protegidos por una clave de acceso.

6.2.3. Depósito de la Clave Privada.

Las claves privadas de los certificados de Security Data están custodiadas por un dispositivo criptográfico, hardware certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multipersona detallado anteriormente. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

Las claves privadas de los certificados de TSU están custodiadas en dispositivos criptográficos seguros certificados con la norma FIPS 140-2 nivel 3.

6.2.4. Copia de Seguridad de la Clave Privada.

Las claves privadas de los certificados de Security Data cuentan con copias de seguridad que permiten su restauración en caso de desastre, pérdida o daño. La generación y recuperación de estas copias se realiza bajo un esquema de control dual, y los ficheros de recuperación se almacenan en armarios ignífugos y en un centro de custodia externo.

6.2.5. Archivo de la Clave Privada del Suscriptor.

Security Data no archivará la clave privada de firma de certificados después de la expiración del periodo de validez de la misma.

Las claves privadas de los certificados internos que usan los distintos componentes del sistema de Security Data para comunicarse entre sí, firmar y cifrar la información serán archivadas por un periodo de al menos 10 años, después de la emisión del último certificado.


6.2.6. Transferencia de la Clave Privada a o desde el Módulo Criptográfico.

Existe un documento de ceremonia de claves de Security Data donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

En otros casos, se podrá utilizar un fichero en formato PKCS12 para transferir la clave privada al módulo criptográfico. En todo caso el fichero estará protegido por un código de activación.

6.2.7. Almacenamiento de clave privada en el módulo criptográfico.

Mediante la aplicación del TSA se valida la librería del módulo criptográfico, se genera el CSR y posterior emisión del certificado en el dispositivo criptográfico.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	38

6.2.8. Método de Activación de la Clave Privada.

Las claves de los certificados de TSA se activan por un proceso que requiere la utilización simultánea dispositivos criptográficos (tarjetas).

6.2.9. Método de Desactivación de la Clave Privada.

La clave privada del TSA de certificados quedará desactivada una vez se elimine del módulo HSM el par de claves.

6.2.10. Método de Destrucción de la Clave Privada.

El método de destrucción se debe regir de acuerdo con lo indicado en el Procedimiento para Archivamiento, Acceso y Destrucción a claves privadas archivadas de Security Data.

6.2.11. Clasificación de modulo Criptográfico.

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas. Para el reinicio se seguirán los pasos descritos en el procedimiento para Eliminación y Destrucción de claves. Finalmente se destruirán de forma segura las copias de seguridad.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.

6.3.1. Archivo de la Clave Pública.


Security Data conservará todas las claves públicas durante el periodo exigido por la legislación vigente, cuando sea aplicable, o mientras el servicio de certificación este activo y 6 meses más como mínimo, en otro caso.

6.3.2. Periodos Operativos de los Certificados y Periodo de uso para el Par de Claves.

El periodo de uso de un certificado será determinado por la validez temporal del mismo.

Un certificado de sellado de tiempo no debe ser usado después del periodo de validez del mismo, aunque la parte que confía pueda usarlo para verificar datos históricos teniendo en cuenta que no existirá un servicio de verificación en línea válido para ese certificado.

6.4. DATOS DE ACTIVACIÓN.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	39

6.4.1. Generación e Instalación de los Datos de Activación.

Los datos de activación son generados en el momento de inicialización del dispositivo criptográfico.

Si la inicialización se produce en una entidad externa, los datos de activación le serán entregados al suscriptor mediante un proceso que asegure la confidencialidad de los mismos ante terceros.

6.4.2. Protección de los Datos de Activación.

Sólo el personal autorizado tiene conocimiento de los datos de activación de las claves privadas de Security Data.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA.

Security Data emplea sistemas fiables y productos comerciales para ofrecer sus servicios de certificación.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Security Data en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Configuración de Usuarios y permisos.
- Configuración de eventos de log.
- Plan de backup y recuperación.
- Configuración antivirus.

La documentación técnica y de configuración de Security Data detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.


6.5.1. Requerimientos Técnicos de Seguridad Específicos.

Cada servidor de Security Data incluye las siguientes funcionalidades:

- Control de acceso a los servicios de TSA y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor y la TSA y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.

Las funcionalidades expuestas son provistas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2. Clasificación de seguridad informática.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	40

Security Data mantiene un inventario de activos y documentación y un procedimiento para la gestión de la información para garantizar su uso.

La política de seguridad detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, INTERNO y CONFIDENCIAL.

6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.

6.6.1. Controles de Desarrollo de Sistemas.

Security Data posee un procedimiento de control de cambios en las versiones y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

6.6.2. Controles de Gestión de Seguridad.

a) Gestión de Seguridad.

Se desarrollan las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un foro para la gestión de la seguridad.

Se exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.


b) Operaciones de Gestión.

Se cuenta con un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

Security Data dispone de cajas de seguridad ignífugas para el almacenamiento de soportes físicos.

Security Data tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

c) Tratamiento de los Soportes y Seguridad.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	41

Todos los soportes serán tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

d) Planning del Sistema.

El departamento técnico de Security Data mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

e) Procedimientos Operacionales y Responsabilidades.

Security Data define actividades asignadas a personas con un rol de confianza distinto a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.3. Controles de seguridad del ciclo de vida.


Gestión del Sistema de Acceso.

Security Data realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el acceso al sistema está limitado a las personas autorizadas. En particular:

- a) Generación del certificado:
 - Las instalaciones de la TSA están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.
 - La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la TSA.

- b) Gestión de la revocación:
 - La revocación se refiere a la pérdida de efectividad de un certificado digital de forma Permanente, certificado en el cual se apoya la TSA. La revocación se realizará mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de TSA.

- c) Estado de la revocación
 - La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	42

Gestión del Ciclo de Vida del Hardware Criptográfico.

- Se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.
- El Hardware criptográfico está construido sobre soportes preparados para evitar cualquier manipulación.
- La TSA registra toda la información pertinente del dispositivo para añadir al catálogo de activos de SECURITY DATA.
- El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.
- SECURITY DATA realiza test de pruebas al menos una vez al año para asegurar el correcto funcionamiento del dispositivo.
- El dispositivo criptográfico solo es manipulado por personal confiable.
- La clave privada del certificado de TSA almacenada en el hardware criptográfico se eliminará una vez se haya retirado el dispositivo.
- Security Data posee un contrato de mantenimiento del dispositivo para su correcto mantenimiento.

6.7. CONTROLES DE SEGURIDAD DE LA RED.

Security Data protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de firewall.

La información confidencial que se trasfiere por redes no seguras se realiza de forma encriptada.


6.8. SELLADO DE TIEMPO.

El servicio de sellado de tiempo de Security Data, proporciona una prueba irrefutable del momento exacto en que se generan documentos electrónicos o se emiten firmas digitales. Este servicio permite demostrar legalmente que un documento existía en un instante específico y que no ha sido alterado posteriormente, incluso cuando el certificado del firmante haya expirado o sido revocado.

Técnicamente, al documento se le aplica una función hash, la cual es enviada a la TSA (Time Stamping Authority). La TSA sella dicho hash con la fecha y hora oficial del servidor y genera un certificado de sellado de tiempo, conforme al estándar RFC 3161, que puede ser adjuntado a la firma digital.

6.8.1. Marco legal en el Ecuador.

De acuerdo con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, las entidades de certificación acreditadas pueden prestar servicios de sellado de tiempo, siempre que estos sean acreditados técnicamente por el ARCOTEL.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	43

El Reglamento de la Ley establece que el sellado de tiempo certifica, para fines legales, la fecha y hora exacta en que un mensaje de datos es recibido y entregado, tomando como referencia el huso horario del territorio continental ecuatoriano. La prestación de este servicio se rige por un esquema de libre competencia y contratación.

6.8.2. Contenido mínimo del sellado de tiempo.

Según la normativa, el sellado de tiempo debe incluir:

- Fecha, expresada en formato año, mes y día.
- Hora, expresada en horas, minutos y segundos conforme al Sistema Internacional de Medidas.
- Identidad, determinada mediante la firma electrónica de la entidad que efectúa el sellado.

6.8.3. Hora legal de referencia.

El servicio de sellado de tiempo utiliza exclusivamente la Hora UTC en todo sus servidores y servicio. En consecuencia, el sellado de tiempo constituye una prueba inequívoca del instante exacto en que un documento electrónico es creado, enviado o recibido.

Security Data garantiza una precisión de sincronización de la hora de la TSA con respecto a la fuente UTC de al menos **+/- 1 segundo**. Para asegurar esta precisión, el sistema utiliza múltiples fuentes de tiempo NTP Stratum 1. En caso de detectarse un *clock drift* (desviación) superior al umbral establecido, el servicio de sellado de tiempo se suspenderá automáticamente para evitar la emisión de sellos con información horaria inexacta, reanudándose únicamente tras una sincronización exitosa y verificada

7. Perfiles del certificado TSA

7.1. PERFIL DE LOS CERTIFICADOS.


Los certificados están alineados con el estándar X.509 versión 3.

Los detalles técnicos, extensiones, campos obligatorios y demás especificaciones del perfil de los certificados se describen en las correspondientes Políticas de Certificación (PC).

7.1.1. Número de versión.

Security Data emite certificados alineados con el estándar X.509 versión 3.

7.1.2. Extensiones de certificado.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	44

Los detalles de las extensiones se encuentran en el perfil de los certificados en las correspondientes Políticas de Certificación (PC).

7.1.3. Identificadores de objetos de algoritmo.

El indicador de objeto del algoritmo de firma es: 1.2.840.113549.1.1.11 SHA-256 with RSA Signature.

7.1.4. Formas de los nombres.

El formato de los nombres se especifica en la correspondiente Política de Certificación.

7.1.5. Restricciones de nombre.

Los nombres contenidos en los certificados son únicos y no ambiguos.

7.1.6. Identificador de objeto de política de certificado.

No es aplicable.

7.1.7. Uso de la extensión Restricciones de política.

No es aplicable.

7.1.8. Sintaxis y semántica de los calificadores de políticas.

No es aplicable.

7.1.9. Semántica de procesamiento para la extensión de políticas de certificados críticos.

No es aplicable.


7.2. PERFIL CRL.

7.2.1. Número(s) de versión.

Las CRL emitidas por Security Data son de la versión 2.

7.2.2. CRL y extensiones de entrada CRL.

Las extensiones de entrada de las CRL se especifican en la Declaración de Prácticas de Certificación de Security Data.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	45

7.3. PERFIL OSCP.

7.3.1. Número(s) de versión.

El perfil OSCP está alineado con el estándar X.509 versión 3.

7.3.2. Extensiones OSCP.

Las extensiones se especifican en la Declaración de Prácticas de Certificación de Security Data.

8. Auditorías de cumplimiento y otros controles.

El sistema de expedición de Certificados de Security Data es sometido a auditorías anuales para garantizar un correcto funcionamiento, operatividad y seguridad.

8.1. FRECUENCIA DE LAS AUDITORIAS.

Se realizarán planes de auditorías internas con presentación de informes, con el fin de tener un control sobre el ciclo de vida de la entidad de certificación y se realizarán auditorías externas siempre y cuando sea solicitado por el ente regulador.

Las auditorías de mantenimiento del sello Webtrust tienen una periodicidad anual.

8.2. CUALIFICACIÓN DEL AUDITOR.

Las auditorías pueden ser de carácter interno o externo. En este segundo caso se realizan por empresas de reconocido prestigio en el ámbito de las auditorías.

8.3. RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA


Las empresas que realizan las auditorías externas nunca representan ningún conflicto de intereses que pueda desvirtuar su actuación en su relación con Security Data.

No obstante, Security Data realizará auditorías internas planificadas con informes mensuales para garantizar en todo momento su adecuación a los requerimientos marcados por las políticas de certificación de la jerarquía.

8.4. ASPECTOS CUBIERTOS POR LOS CONTROLES

La auditoría verifica los siguientes principios:

- a) **Publicación de la Información:** Que Security Data hace públicas las Prácticas de Negocio y de Gestión de Certificados (la presente DPC), así como la política de privacidad de la información y protección de datos personales y proporciona sus servicios en

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	46

conformidad con dichas afirmaciones.

- b) Integridad de Servicio. Que Security Data mantiene controles efectivos para asegurar razonablemente que:
- La información del suscriptor es autenticada adecuadamente (para las actividades de registro realizadas), y
- c) Controles generales. Que Security Data mantiene controles efectivos para asegurar razonablemente que:
- La información de suscriptores y usuarios está restringida a personal autorizado y protegida de usos no especificados en las prácticas de negocio de la TSA publicadas.
 - Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las claves y los certificados.
 - Las tareas de explotación, desarrollo y mantenimiento de los sistemas de Security Data son adecuadamente autorizadas y realizadas para mantener la integridad de los mismos.

8.5. ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE INCIDENCIAS.

En caso de que sean detectadas incidencias o no-conformidades, se habilitarán las medidas oportunas para su resolución en el menor tiempo posible. Security Data se compromete a su resolución en un plazo máximo de sesenta días.

En todo caso se formará un comité de resolución formado por personal de las áreas afectadas y otro de seguimiento formador por los responsables de las áreas afectadas y Dirección General.

8.6. COMUNICACIÓN DE RESULTADOS.

El auditor comunicará los resultados a la alta gerencia y al sistema de gestión.


9. Otras cuestiones legales y de actividad.

9.1. TARIFAS.

9.1.1. Tarifa de emisión o renovación de certificados.

La tarifa correspondiente a la emisión o renovación de Sellos de Tiempo se encuentra vinculada a los precios establecidos para las firmas electrónicas, los cuales pueden ser consultados en el siguiente enlace oficial:

https://www.securitydata.net.ec/firma-electronica-en-ecuador/#planes_fe

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	47

Al momento de la emisión del certificado, se procederá a realizar una cotización personalizada, acorde a las necesidades específicas del cliente y a las condiciones vigentes.

La tarifa está sujeta a revisión o modificación sin previo aviso, por parte de gerencia o el departamento comercial de SECURITY DATA, de igual manera los precios pueden ser variables teniendo en cuenta promociones o normativas legales vigentes en el país.

9.1.2. Tarifas de Acceso a los Certificados de Sellado de tiempo.

El acceso a la clave pública de los certificados de sellado de tiempo emitidos es gratuito, no obstante, Security Data se reserva el derecho de imponer alguna tarifa debido a cambios legales o cualquier otra circunstancia que a juicio de Security Data deba ser gravada.

9.1.3. Tarifas de Acceso a la Información de Estado o Revocación.

Security Data provee un acceso a la información relativa al estado de los certificados de sellado de tiempo gratuito, por medio de la publicación de las correspondientes CRL.

Security Data ofrece otros servicios de validación de certificados comerciales (como OCSP).

9.1.4. Tarifas de Otros Servicios.

Las tarifas aplicables a otros servicios se negociarán entre Security Data y los clientes de los servicios ofrecidos.

9.1.5. Política de Reembolso.

Los suscriptores de certificados podrán solicitar reembolso de dinero bajo los siguientes lineamientos:

- Cuando se haya realizado un depósito en exceso
- Cuando el servicio no ha sido proporcionado y el cliente no desea seguir con el trámite


Para estos casos el cliente deberá demostrar las evidencias del pago realizado, una vez analizadas las circunstancias para efectuar el reembolso el departamento financiero procederá con la devolución respectiva.

En estos casos el cliente debe enviar un correo electrónico indicando el motivo del reembolso a devoluciones@securitydata.net.ec, una vez analizado si aplica o no el reembolso se procede a comunicar al cliente.

El valor del reembolso será el del servicio solicitado, y el valor depositado en exceso.

9.2. RESPONSABILIDADES FINANCIERAS.

9.2.1. Cobertura del Seguro.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	48

El seguro cubre todos los perjuicios contractuales y extracontractuales de los clientes de Security Data, exenta de culpa de derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la Entidad de Certificación SECURITY DATA en el desarrollo de las actividades para las cuales cuenta con autorización.

9.2.2. Otros Bienes.

Sin estipulación

9.2.3. Seguro o Garantía de Cobertura para las Entidades Finales.

Security Data ha adquirido un seguro expedido por una entidad aseguradora autorizada para operar en Ecuador, que cubre todos los perjuicios contractuales y extracontractuales de los titulares y Terceros que confían exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de Security Data en el desarrollo de las actividades para las cuales cuenta con autorización.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN.

Security Data dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo que deberán firmar todas las personas que tengan acceso a información confidencial ya sea esta comercial, técnica, operativa, recursos humanos, etc.

9.3.1. Alcance de la Información Confidencial.

Toda información no pública es considerada confidencial y por tanto de acceso restringida:


Confidencialidad de la clave privada de la Entidad de Certificación.

- Confidencialidad de la clave privada del titular.
- Confidencialidad de la información suministrada por el titular.
- Registros de las transacciones.
- Registros de pistas de Auditoría.
- Políticas de seguridad.
- Plan de Contingencia.
- Planes de continuidad del negocio.
- Cualquier otra información relacionada con el suscriptor o Security Data que puede ser de naturaleza confidencial.

9.3.2. Información No Confidencial.

La siguiente información se considerará como no confidencial:

- La contenida en la presente DPC.
- Toda la información contenida en los certificados emitidos y listas de revocación de

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	49

certificados (CRL), incluyendo toda la información que se pueda obtener de este tipo.

- Información de los certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) e información de los estados de certificados.
- Cualquier información cuya publicidad sea impuesta normativamente.
- Toda la información clasificada expresamente como "PÚBLICA".

9.3.3. Responsabilidad de proteger la información confidencial.

Los empleados, agentes y contratistas de Security Data están obligados contractualmente a proteger la información confidencial.

Los suscriptores de certificados son responsables de proteger su propia clave privada y toda la información de activación (es decir, contraseñas o PIN) necesarios para acceder o utilizar la clave privada.

9.4. PRIVACIDAD DE LA INFORMACIÓN PERSONAL.

9.4.1. Política de Privacidad.

Security Data tiene como política de privacidad lo establecido en el derecho de habeas data: “La información privada, será aquella que por versar sobre información personal o no, y que, por encontrarse en un ámbito privado, solo puede ser obtenida u ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones.”

9.4.2. Información tratada como Privada.

La información personal acerca de un individuo que no está disponible públicamente en el contenido de un certificado o del CRL se considera privada.


En cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPD), Security Data garantiza a los titulares el ejercicio de sus derechos de acceso, rectificación y oposición. Una vez cumplido el plazo legal de conservación de 15 años exigido por la Ley de Comercio Electrónico para fines de prueba, Security Data procederá a la eliminación segura de los datos personales de sus bases de datos operativas, o a su anonimización irreversible, manteniendo únicamente la información técnica estadística que no permita la identificación del titular.

9.4.3. Información No Calificada como Privada.

El contenido del certificado y la información del estado del certificado no se consideran privados.

9.4.4. Responsabilidad de la Protección de los Datos de Carácter Personal.

Security Data es responsable y cuenta con los adecuados mecanismos de seguridad y control para asegurar la protección, confidencialidad y debido uso de la información suministrada por el titular.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	50

9.4.5. Notificación y Consentimiento para usar Datos de Carácter Personal.

Los datos de carácter personal no podrán ser comunicados o usados por terceros, sin la debida notificación y consentimiento del titular.

9.4.6. Revelación en el marco de un proceso administrativo o judicial.

Security Data puede divulgar información privada sin previo aviso a los solicitantes o suscriptores cuando dicha divulgación sea requerida por ley o regulación.

9.4.7. Otras circunstancias de revelación de información.

No es aplicable.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL.

Security Data, tiene derechos de propiedad intelectual sobre todos sus documentos normativos, planes, procesos, patentes, marca comercial, material comercial y certificados que emita si no se acuerda explícitamente lo contrario, y no podrán ser modificados o atribuidos a otra entidad de manera no autorizada.

9.6. DECLARACIONES Y GARANTÍAS.

9.6.1. Declaraciones y Garantías de CA.

Security Data representa, en la medida especificada en su PC / DPC, cumple, en todos los aspectos materiales, con todas las leyes y regulaciones aplicables.

Security Data asegura que:


- Ha tomado medidas razonables para verificar que la información contenida en cualquier Certificado sea precisa en el momento de la emisión y se verifique de acuerdo con este documento.
- Los certificados se revocarán si Security Data cree o se le notifica que el contenido del certificado ya no es exacto, o que la clave asociada con un certificado se ha visto comprometida de alguna manera.

Security Data no ofrece otras garantías, y todas las garantías, expresas o implícitas, legales o de otro tipo, están excluidas en la mayor medida permitida por la ley aplicable, incluidas, entre otras, todas las garantías en cuanto a comerciabilidad o idoneidad para un propósito particular.

9.6.2. Declaraciones y Garantías de RA.

Security Data garantiza que:

- Lleva a cabo el proceso de emisión de conformidad con este documento.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	51

- La información proporcionada no contiene ninguna información falsa o engañosa.
- Todos los certificados de sellado de tiempo solicitados cumplen con todos los requisitos materiales de este documento.

9.6.3. Representación y Garantías del Suscriptor.

Los suscriptores representan y garantizan a Security Data, a los terceros que confían y otras partes que, para cada certificado, el suscriptor debe:

- Generar de forma segura sus claves privadas y proteger su clave privada.
- Proporcionar información precisa y completa cuando se comunique con Security Data.
- Confirmar la exactitud de los datos del certificado antes de usarlo.
- Solicitar de inmediato la revocación de un Certificado y notificar a Security Data si hay algún compromiso real o sospechoso de la Clave Privada asociada con la Clave Pública incluida en el certificado.
- Solicitar inmediatamente la revocación del Certificado y dejar de usarlo, si alguna información en el Certificado es o se vuelve incorrecta o inexacta.
- Usar el Certificado solo para fines autorizados y legales, de acuerdo con el propósito del certificado, esta DPC, cualquier PC aplicable y el Acuerdo de Suscriptor relevante.
- Dejar de usar el Certificado y la Clave privada relacionada inmediatamente después de la fecha de vencimiento del Certificado.

9.6.4. Representación y Garantías del Tercero que Confía.

El tercero que confía es el único responsable de tomar la decisión de confiar en un certificado de Security Data.

9.6.5. Representación y Garantías de Otras Partes.

No es aplicable.


9.7. RENUNCIAS DE GARANTÍAS.

El servicio de sellado de tiempo se presta sin garantías implícitas adicionales, limitándose a lo expresamente establecido en la presente DPC y en la normativa aplicable.

9.8. LIMITACIONES DE RESPONSABILIDAD.

En la medida en que Security Data, haya emitido y administrado el certificado de sellado de tiempo de acuerdo con la DPC, no tendrá ninguna responsabilidad ante el Suscriptor, el tercero que confía o cualquier Tercero por cualquier pérdida o daño sufrido como resultado del uso o dependencia de dicho certificado.

Security Data no asume ninguna responsabilidad con respecto a la monitorización del contenido, tipo y/o formato de los documentos donde se utilice el servicio de sellado de tiempo.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	52

9.9. INDEMNIZACIONES.

Los casos de indemnización son definidos en los contratos de los titulares.

9.10. VIGENCIA Y TERMINACIÓN.

9.10.1. Vigencia.

Este documento de Declaración de Prácticas de Certificación de Sellado de Tiempo y cualquier enmienda a este, entrarán en vigencia tras su publicación en la web de Security Data y permanecerán vigentes hasta que sea reemplazado por una versión nueva.

9.10.2. Terminación.

Este documento de Declaración de Prácticas de Certificación de Sellado de Tiempo y cualquier enmienda permanecerán en vigor hasta que se modifique o reemplace por una versión nueva.

9.10.3. Efecto de la Terminación y la Supervivencia.

Al finalizar esta Declaración de Prácticas de Certificación de Sellado de Tiempo, los participantes de SECURITY DATA están sujetos a sus términos para todos los certificados emitidos por el resto de los períodos de validez de dichos certificados. Como mínimo, todas las responsabilidades relacionadas con la protección de la información confidencial sobrevivirán a la terminación.

9.11. NOTIFICACIÓN INDIVIDUALES Y COMUNICACIÓN.

De modo general, se utilizará el sitio web de SECURITY DATA para realizar cualquier tipo de notificación y comunicación. En caso de problemas de seguridad o de pérdida de integridad que puedan afectar a una persona física o jurídica, SECURITY DATA notificará a ésta dicha incidencia.

9.12. ENMIENDAS.

Las enmiendas y cambios serán comunicadas a la ARCOTEL y luego de su aprobación serán publicadas en la página web y notificadas a los titulares y suscriptores, conforme a los medios especificados en sus contratos.


9.12.1. Procedimiento de modificación.

No es aplicable.

9.12.2. Mecanismo y plazo de notificación.

No es aplicable.

9.12.3. Circunstancias en las que se debe cambiar el OID.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	53

No es aplicable.

9.13. PROCEDIMIENTO DE RESOLUCIÓN DE DISPUTAS.

El procedimiento de resolución de disputas será definido en los contratos de los titulares.

9.14. CONFORMIDAD CON LA LEY APLICABLE.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento; Ley Orgánica de Defensa del consumidor, Ley Orgánica de Transparencia de la Información y Acreditación de ARCOTEL.

9.15. CUMPLIMIENTO DE LA LEY APLICABLE.

Los certificados emitidos bajo SECURITY DATA serán utilizados por los suscriptores y terceros que confían solo de acuerdo con las leyes y reglamentos de la jurisdicción en la que se utilizan o se basan.

9.16. PROVISIONES MISCELÁNEAS.

9.16.1. Acuerdo Completo.

Sin estipulación.

9.16.2. Asignación.

Las TSA emisoras, los suscriptores, los terceros que confían, las Entidades de registro o cualquier otra entidad que opere bajo esta Declaración de Prácticas de Certificación no tienen derecho a asignar ninguno de sus derechos u obligaciones bajo esta Declaración de Prácticas de Certificación.


9.16.3. Divisibilidad.

Si alguna de las disposiciones de esta Declaración de Prácticas de Certificación se considera inválida por una autoridad competente en la jurisdicción aplicable, el resto de la Declaración de Prácticas y Política de Certificación seguirá siendo válido y exigible.

9.16.4. Ejecución.

Sin estipulación.

9.16.5. Fuerza mayor.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO	CÓDIGO	SD-ID-PE-14
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	54

Security Data no acepta ninguna responsabilidad por cualquier retraso o incumplimiento de una obligación en virtud de su Declaración de Prácticas de Certificación en la medida en que dicho retraso o incumplimiento sea causado por eventos que escapen a su control razonable.

9.17. OTRAS PROVISIONES.

Sin estipulación.

10. Control de aprobaciones

ELABORADO POR	SUPERVISOR LEGAL	
REVISADO POR	CHIEF TECHNOLOGY OFFICER (CTO)	
APROBADO POR	GERENTE GENERAL	