

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	1



POLÍTICA DE
CERTIFICACIÓN DE
SELLO DE TIEMPO

febrero 13

2026

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		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	22/12/2025	SUPERVISOR LEGAL	CHIEF TECHNOLOGY OFFICER (CTO)	GERENTE GENERAL
2	Actualización general de la PC conforme a la Normativa Técnica y RFC 3647.	13/02/2026	SUPERVISOR LEGAL	CHIEF TECHNOLOGY OFFICER (CTO)	GERENTE GENERAL

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	3

Contenido

1.	Introducción.....	9
1.1.	DESCRIPCIÓN GENERAL.....	9
1.2.	NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO.	9
1.3.	PARTICIPANTES DE LA PKI.	10
1.3.1.	Autoridad de Certificación.	10
1.3.2.	Prestador de Servicios de Certificación.....	10
1.3.3.	Autoridad de Sellado de Tiempo.....	10
1.3.4.	Suscriptores.....	10
1.3.5.	Partes que Confían.	10
1.4.	USO DEL CERTIFICADO.	10
1.4.1.	Usos apropiados del Certificado.	10
1.4.2.	Usos Prohibidos de los Certificados.	11
1.5.	ADMINISTRACIÓN DE POLÍTICAS.....	11
1.5.1.	Organización que administra el Documento.....	11
1.5.2.	Persona de Contacto.	11
1.5.3.	Persona que determina la idoneidad del CPS para la Política.....	12
1.5.4.	Procedimientos de aprobación de la CPS.....	12
1.6.	DEFINICIONES Y ACRÓNIMOS.	12
1.6.1.	Definiciones.....	12
1.6.2.	Acrónimos.	13
2.	Responsabilidades de Publicación y Repositorio.	14
2.1.	REPOSITORIOS.....	14
2.2.	PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN.	14
2.3.	TIEMPO O FRECUENCIA DE PUBLICACIÓN.	14
2.4.	CONTROLES DE ACCESO A LOS REPOSITORIOS.	14
3.	Identificación y Autenticación.....	14
3.1.	DENOMINACIÓN.	14
3.1.1.	Tipos de Nombres.	15
3.1.2.	Necesidad de que los nombres tengan significado.....	15
3.1.3.	Anonimato o seudónimo de los suscriptores.....	15
3.1.4.	Reglas para la Interpretación de las distintas formas de nombres.....	15

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	4

3.1.5.	Unicidad de los nombres.....	15
3.1.6.	Reconocimiento, autenticación y función de las marcas.....	15
3.2.	VALIDACIÓN DE IDENTIDAD INICIAL.....	16
3.2.1.	Método para demostrar la posesión de la clave privada.....	16
3.2.2.	Autenticación de la Identidad de la Organización.....	16
3.2.3.	Autenticación de la Identidad Individual.....	16
3.2.4.	Información de suscriptor no verificada.....	16
3.2.5.	Validación de la Autoridad.....	16
3.2.6.	Criterios de Interoperabilidad.....	17
3.3.	IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN DE CLAVES.	17
3.3.1.	Identificación y Autenticación para la renovación rutinaria de claves.....	17
3.3.2.	Identificación y Autenticación para la renovación de claves después de la revocación.....	17
3.4.	IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA SOLICITUD DE REVOCACIÓN.....	17
4.	Requisitos Operacionales del Ciclo de Vida del Certificado.....	17
4.1.	SOLICITUD DEL CERTIFICADO.....	17
4.2.	PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES.....	18
4.3.	EMISIÓN DEL CERTIFICADO.....	18
4.4.	ACEPTACIÓN DEL CERTIFICADO.....	18
4.5.	USO DE PARES DE CLAVES Y CERTIFICADOS.....	18
4.6.	RENOVACIÓN DEL CERTIFICADO.....	18
4.7.	CAMBIO DE CLAVE DEL CERTIFICADO.....	18
4.8.	MODIFICACIÓN DEL CERTIFICADO.....	18
4.9.	REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO.....	18
4.10.	SERVICIOS DE ESTADO DE CERTIFICADOS.....	18
4.11.	FIN DE LA SUSCRIPCIÓN.....	18
4.12.	CUSTODIA Y RECUPERACIÓN DE CLAVES.....	19
5.	Controles de Instalaciones, Gestión y Operación.....	19
5.1.	CONTROLES FÍSICOS.....	19
5.2.	CONTROLES DE PROCEDIMIENTO.....	19
5.2.1.	Roles de Confianza.....	19
5.3.	CONTROLES DE PERSONAL.....	19

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	5

5.3.1.	Calificaciones, Experiencia y Requisitos.....	19
5.3.2.	Comprobación de Antecedentes.....	19
5.3.3.	Requisitos de formación.....	20
5.3.4.	Frecuencia y requisito de reentrenamiento.....	20
5.3.5.	Frecuencia y requisito de reentrenamiento.....	20
5.3.6.	Sanciones por acciones no autorizadas.....	20
5.3.7.	Requisitos del contratista independiente.	20
5.3.8.	Documentación suministrada al Personal.....	21
5.4.	PROCEDIMIENTOS DE REGISTRO DE AUDITORÍA.....	21
5.4.1.	Tipos de Eventos Registrados.....	21
5.4.2.	Frecuencia de Procesado de Registros de Auditoría.....	21
5.4.3.	Periodo de Conservación de los Registros de Auditoría.	22
5.4.4.	Protección de los Registros.	22
5.4.5.	Procedimientos de Respaldo de los Registros de Auditoría.....	22
5.4.6.	Sistema de Recolección de Información de Auditoría.	22
5.4.7.	Notificación de Eventos.....	22
5.4.8.	Análisis de Vulnerabilidades.....	23
5.5.	ARCHIVO DE REGISTRO.	23
5.5.1.	Tipo de Registros Archivados.	23
5.5.2.	Periodo de conservación de los datos.....	23
5.5.3.	Protección del Archivo.	23
5.5.4.	Procedimientos de Copia de Seguridad del Archivo.	23
5.5.5.	Requerimientos para el Sellado de Tiempo de los Registros.....	23
5.5.6.	Sistema de Archivo de Información de Auditoría.	24
5.6.	CAMBIO DE CLAVE.....	24
5.7.	COMPROMISO Y RECUPERACIÓN ANTE DESASTRES.....	24
5.7.1.	Procedimientos de Manejo de Incidentes y Compromisos.	24
5.7.2.	Recursos Informáticos, software y/o datos.	24
5.7.3.	Procedimiento de compromiso de Clave Privada de la entidad.	24
5.7.4.	Capacidades de Continuidad de Negocio después de un Desastre.	24
5.8.	TERMINACIÓN O CESE.....	24
6.	Controles Técnicos de Seguridad.	25
6.1.	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.	25

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	6

6.2.	PROTECCIÓN DE CLAVES PRIVADAS E INGENIERÍA DE MÓDULOS CRIPTOGRÁFICOS.	25
6.3.	OTROS ASPECTOS DE LA GESTIÓN DE PARES DE CLAVES.....	25
6.4.	DATOS DE ACTIVACIÓN.	25
6.5.	CONTROLES DE SEGURIDAD INFORMÁTICA.....	25
6.6.	CONTROLES TÉCNICOS DEL CICLO DE VIDA.	26
6.7.	CONTROLES DE SEGURIDAD DE LA RED.	26
6.8.	SELLADO DE TIEMPO.	26
6.8.1.	Tipos y Usos de los Sellos de Tiempo.	26
6.8.2.	Validación de los Sellos de Tiempo.	26
6.8.3.	Exactitud de la Hora en el Sello de Tiempo.....	27
6.8.4.	Límites de Uso del Certificado.....	27
7.	Perfiles de Certificados, CRL y OCSP.	27
7.1.	PERFIL DEL CERTIFICADO.....	27
7.1.1.	Número de Versión.	30
7.1.2.	Extensiones del Certificado.	30
7.1.3.	Identificadores de Objetos de Algoritmos.	30
7.1.4.	Formas de los nombres.	30
7.1.5.	Restricciones de Nombre.	30
7.1.6.	Identificador de objeto de Política de Certificado.	30
7.1.7.	Uso de la extensión Restricciones de Política.	30
7.1.8.	Sintaxis y Semántica de los calificadores de Política.....	31
7.1.9.	Semántica de procesamiento para la Extensión de Políticas de Certificados Críticos.	31
7.2.	PERFIL CRL.	31
7.2.1.	Número de Versión.	31
7.2.2.	CRL y extensiones de entrada CRL.	31
7.3.	PERFIL OCSP.	31
7.3.1.	Número de Versión.	32
7.3.2.	Extensiones OCSP.....	32
8.	Auditorías de cumplimiento y otros controles.....	33
8.1.	FRECUENCIA DE LAS AUDITORIAS.	33
8.2.	CUALIFICACIÓN DEL AUDITOR.	33
8.3.	RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA.....	33

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	7

8.4.	ASPECTOS CUBIERTOS POR LOS CONTROLES.....	34
8.5.	ACCIONES ADOPTADAS COMO RESULTADO.....	34
8.6.	COMUNICACIÓN DE RESULTADOS.	34
9.	Otros Asuntos Comerciales y Legales.....	34
9.1.	TARIFAS.	34
9.1.1.	Tarifas de Emisión o Renovación de certificados.....	35
9.1.2.	Tarifas de acceso al certificado.	35
9.1.3.	Tarifas de Acceso a la Información de revocación o estado.	35
9.1.4.	Tarifa por Otros Servicios.....	35
9.1.5.	Política de Reembolso.....	35
9.2.	RESPONSABILIDAD FINANCIERA.....	35
9.2.1.	Cobertura del Seguro.	35
9.2.2.	Otros Bienes.	35
9.2.3.	Seguro o Garantía de Cobertura para las Entidades Finales.....	36
9.3.	CONFIDENCIALIDAD DE LA INFORMACIÓN EMPRESARIAL.....	36
9.3.1.	Alcance de la Información Confidencial.....	36
9.3.2.	Información No Confidencial.....	36
9.3.3.	Deber de Proteger la Información Confidencial.....	37
9.4.	PRIVACIDAD DE LA INFORMACIÓN PERSONAL.....	37
9.4.1.	Política de Privacidad.	37
9.4.2.	Información tratada como Privada.	37
9.4.3.	Información No Calificada como Privada.....	37
9.4.4.	Responsabilidad de la Protección de los Datos de Carácter Personal.	37
9.4.5.	Notificación y Consentimiento para usar Datos de Carácter Personal.....	37
9.4.6.	Revelación en el marco de un proceso administrativo o judicial.....	37
9.4.7.	Otras circunstancias de revelación de información.	38
9.5.	DERECHOS DE PROPIEDAD INTELECTUAL.....	38
9.6.	DECLARACIONES Y GARANTÍAS.....	38
9.6.1.	Declaraciones y Garantías de la CA.....	38
9.6.2.	Declaraciones y Garantías de la RA.	38
9.6.3.	Declaraciones y Garantías de los Suscriptores.....	39
9.6.4.	Declaraciones y Garantías de la parte que Confía.	39
9.6.5.	Declaraciones y Garantías de Otros Participantes.....	40

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	8

9.7.	RENUNCIAS A GARANTÍAS.....	40
9.8.	LIMITACIONES DE RESPONSABILIDAD.....	40
9.9.	INDEMNIZACIONES.	41
9.10.	PLAZO Y TERMINACIÓN.....	41
9.10.1.	Plazo.....	41
9.10.2.	Terminación.....	41
9.11.	AVISOS Y COMUNICACIONES INDIVIDUALES CON LOS PARTICIPANTES.....	41
9.12.	ENMIENDAS.....	41
9.13.	DISPOSICIONES DE RESOLUCIÓN DE DISPUTAS.	41
9.14.	LEY APLICABLE.	41
9.15.	CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE.....	41
9.16.	DISPOSICIONES DIVERSAS.	42
9.16.1.	Acuerdo Completo.	42
9.16.2.	Cesión.....	42
9.16.3.	Divisibilidad.	42
9.16.4.	Ejecución.	42
9.16.5.	Fuerza Mayor.	42
9.17.	OTRAS DISPOSICIONES.....	42
10.	Control de Versiones.....	42

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	9

1. Introducción.

1.1. DESCRIPCIÓN GENERAL.

Security Data Seguridad en Datos y Firma Digital S.A. es una entidad certificadora que nació con el fin de cubrir las necesidades del mercado ecuatoriano de firma electrónica y certificados digitales.

Security Data Seguridad en Datos y Firma Digital S.A. es una empresa constituida de acuerdo a la legislación ecuatoriana, inscrita en el registro mercantil bajo el número 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 Seguridad en Datos y Firma Digital S.A. están orientados a Personas particulares, Corporaciones Públicas y Privadas (como empresas, entidades públicas) cuyo objetivo es acreditar la identidad digital de las corporaciones y las personas naturales que actúan a través de la red.

En el presente documento se declara la Política de Certificación para el servicio de sellado de Tiempo de Security Data Seguridad en Datos y Firma Digital S.A., en adelante Security Data, dando cumplimiento a las normas y decretos aplicables a la prestación de servicios de certificación digital.

La Política de Certificación es de cumplimiento obligatorio para la CA, su personal, proveedores y demás partes que intervengan en la prestación del servicio de sellado de tiempo, y constituye un documento público, salvo aquellas secciones que, por razones de seguridad, deban ser clasificadas.

Esta Política de Certificación (PC), junto con la DPC de sello de tiempo de la EC Security Data Seguridad en Datos y Firma Digital S.A., están dirigidas a cualquiera que confíe en este tipo de certificados.

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO.

Nombre:	Política de Certificación de Sello de Tiempo
Código del documento:	SD-ID-PE-12
Versión:	2
Descripción:	Política de Certificación de Sello de Tiempo de Security Data Seguridad en Datos y Firma Digital S.A.
Fecha de publicación:	12 de febrero del 2026
Tipo de documento:	Público
OID:	1.3.6.1.4.1.37746.102.2.5.1

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	10

1.3. PARTICIPANTES DE LA PKI.

1.3.1. Autoridad de Certificación.

La Autoridad de Certificación, en adelante “AC” es la persona autorizada y facultada para emitir certificados en relación con las firmas electrónicas de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas electrónicas.

1.3.2. Prestador de Servicios de Certificación.

El Prestador de Servicios Electrónicos de Certificación (PSC) es la persona, 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.

1.3.3. Autoridad de Sellado de Tiempo.

Security Data es el Prestador de Servicios de Certificación que actúa como Autoridad de Sellado de Tiempo (TSA) para la emisión de sellos de tiempo y certificados de sellos de tiempo electrónicos.

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. Partes 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. USO DEL CERTIFICADO.

1.4.1. Usos apropiados del Certificado.

Estos certificados deberán utilizarse en conformidad con la normativa legal vigente, reguladora de determinados aspectos de los servicios electrónicos de confianza. El uso de las claves y el certificado por parte del suscriptor presupone la aceptación de las condiciones de uso establecidas en la DPC de Sello de Tiempo de Security Data.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	11

Se considerará que se hace un uso indebido de un certificado cuando éste sea utilizado para realizar operaciones no autorizadas según la presente Política de Certificación (PC) aplicable al certificado y los contratos con sus suscriptores, consecuencia de esto, Security Data podrá revocar el certificado y dar por terminado el contrato de manera unilateral.

Si el certificado del suscriptor en el período de vigencia se encontrara comprometido, es decir su clave privada, deberá iniciar el procedimiento de revocación como se lo menciona en esta PC y DPC.

1.4.2. Usos Prohibidos de los Certificados.

No se permite el uso que sea contrario a la normativa ecuatoriana y comunitaria, a los convenios internacionales ratificados por el estado ecuatoriano, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta Política de Certificación y en las DPC establecidas.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Los certificados de usuario final no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados.

1.5. ADMINISTRACIÓN DE POLÍTICAS.

1.5.1. Organización que administra el Documento.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. es la entidad que administra y es autora de la presente Política de Certificación y otros documentos normativos.

1.5.2. Persona de Contacto.

Nombre:	Lenin Alberto Vásquez Gonzalez
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

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	12

1.5.3. Persona que determina la idoneidad del CPS para la Política.

El presente documento es firmado digitalmente por el Responsable de la AC de Security Data antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

1.5.4. Procedimientos de aprobación de la CPS.

La publicación de las revisiones de esta PC y DPC, deben ser aprobados y firmados por el responsable de la AC de Security Data antes de su publicación.

Las versiones actualizadas y aprobadas de las PC, así como de los demás documentos normativos, serán remitidas a la Autoridad de Control y, posteriormente, publicadas en la página web de Security Data.

Cada documento mantendrá un historial de versiones, en el cual se registrarán los cambios efectuados, con el fin de prevenir alteraciones no autorizadas o suplantaciones.

1.6. DEFINICIONES Y ACRÓNIMOS.

1.6.1. Definiciones.

ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones.

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.

Sistemas de la TSA: Sistemas de tecnologías de la información que soportan la provisión de servicios de sellado de tiempo. Componentes de hardware y software que son administrados como una unidad para proveer sellos de tiempo desde una fuente de tiempo.

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

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	13

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 Transformación Format – 8 bits.
TSU:	Unidad de Sellado de Tiempo.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	14

2. Responsabilidades de Publicación y Repositorio.

2.1. REPOSITORIOS.

Declaración de Practicas de Certificación de sello de tiempo:

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

Política de Certificación:

<https://www.securitydata.net.ec/normativas/pcsellotiempo.pdf>

Certificado CA Raíz:

https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SECDATA-CA-2.cer

Certificado CA Subordinada:

<http://subca2.securitydata.net.ec/subca2sd/subca2.crt>

CRL:

- <http://crl1.securitydata.net.ec/subca2crl1/crlfile.crl>
- <http://crl2.securitydata.net.ec/subca2crl2/crlfile.crl>

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN.

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

2.3. TIEMPO O FRECUENCIA DE PUBLICACIÓN.

La presente PC de Sellado de Tiempo serán revisadas y si procede, actualizadas, anualmente o cuando se presente o requiera algún cambio.

Cualquier cambio sustancial que afecte la confianza o la operatividad será notificado a la autoridad de control (ARCOTEL) con al menos 15 días de antelación a su publicación.

2.4. CONTROLES DE ACCESO A LOS REPOSITORIOS.

La consulta a los repositorios disponibles en la página web de Security Data antes mencionados, es de libre acceso al público.

3. Identificación y Autenticación.

3.1. DENOMINACIÓN.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	15

3.1.1. Tipos de Nombres.

Todos los certificados 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:

- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles.
- RFC 5280 " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

3.1.2. Necesidad de que los nombres tengan significado.

Security Data garantizará que los nombres asignados en los certificados digitales, tanto del titular (Subject) como del emisor (Issuer), sean significativos, claros, precisos y no ambiguos, de conformidad con la Norma Técnica.

Los nombres utilizados deberán identificar de forma explícita a la persona jurídica o entidad titular y garantizando que el uso del sello de tiempo pueda ser atribuido de manera objetiva a la entidad correspondiente.

3.1.3. Anonimato o seudónimo de los suscriptores.

No se podrán utilizar alias en los campos de Titular, Security Data no emite certificados con seudónimos.

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

El nombre del titular del certificado deberá corresponder exactamente a la denominación legal o institucional que conste en los documentos oficiales presentados durante el proceso de validación.

Los nombres incluidos en los campos de identificación del certificado deberán permitir la identificación inequívoca del titular del certificado de sello de tiempo, sin ambigüedades ni elementos que puedan inducir a error respecto de su identidad, naturaleza jurídica o ámbito de actuación.

3.1.5. Unicidad de los nombres.

El DN de los certificados emitidos es único para cada suscriptor y/o firmante. Sin embargo, para una misma persona que disponga de varios certificados y tipos de certificados se dispone de un serial únicos por cada uno.

3.1.6. Reconocimiento, autenticación y función de las marcas.

 <p>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	16

La AC no está obligada a recopilar o solicitar evidencia en relación con la posesión o titularidad de marcas registradas u otros signos distintivos antes de la emisión de los certificados. Security Data no asume ninguna obligación en la emisión de certificados respecto al uso de marcas registradas u otros signos distintivos.

3.2. VALIDACIÓN DE IDENTIDAD INICIAL.

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 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.

Según lo definido en la DPC de Sello de Tiempo.

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.

No aplicable.

3.2.4. Información de suscriptor no verificada.

Bajo ninguna circunstancia Security Data omitirá las tareas de verificación que conduzcan a la identificación del Suscriptor y que se traduce en la solicitud de exhibición de los documentos mencionados para personas jurídicas.

3.2.5. Validación de la Autoridad.

La AC verifica que el solicitante del certificado posea la autoridad, facultad o representación legal necesaria para actuar en nombre de la persona jurídica, cargo o función al que estará asociado el certificado solicitado.

La AC valida que el solicitante cuente con un nombramiento, poder o autorización vigente, otorgado conforme a la normativa legal aplicable, que lo faculte para solicitar y utilizar el certificado en representación de la entidad, en concordancia con lo indicado en el apartado Autenticación de la Identidad de una Persona Jurídica.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	17

3.2.6. Criterios de Interoperabilidad.

Security Data emite certificados de sello de tiempo conforme a estándares técnicos internacionalmente reconocidos, garantizando su interoperabilidad y posibilidad de validación por parte de sistemas, aplicaciones y terceros que confían, disponen también del certificado raíz y subordinado configurado.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN DE CLAVES.

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. 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 aplicable.

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

No aplicable.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA SOLICITUD DE REVOCACIÓN.

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 Operacionales del Ciclo de Vida del Certificado.

4.1. SOLICITUD DEL CERTIFICADO.

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

 <p>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<p>POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO</p>	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	18

4.2. PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES.

El proceso de tramitación se realizará según lo definido en la DPC de sello de tiempo de Security Data.

4.3. EMISIÓN DEL CERTIFICADO.

El proceso de emisión se realizará según lo definido en la DPC de sello de tiempo de Security Data.

4.4. ACEPTACIÓN DEL CERTIFICADO.

El proceso de aceptación se realizará según lo definido en la DPC de sello de tiempo de Security Data.

4.5. USO DE PARES DE CLAVES Y CERTIFICADOS.

El proceso se realizará según lo definido en la DPC de sello de tiempo de Security Data.

4.6. RENOVACIÓN DEL CERTIFICADO.

El proceso de renovación se realizará según lo definido en la DPC de sello de tiempo de Security Data.

4.7. CAMBIO DE CLAVE DEL CERTIFICADO.

No es aplicable

4.8. MODIFICACIÓN DEL CERTIFICADO.

El proceso de solicitud se realizará según lo definido en la DPC de sello de tiempo de Security Data.

4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO.

El proceso de solicitud se realizará según lo definido en la DPC de sello de tiempo de Security Data.

4.10. SERVICIOS DE ESTADO DE CERTIFICADOS.

El proceso se realizará según lo definido en la DPC de sello de tiempo de Security Data.

4.11. FIN DE LA SUSCRIPCIÓN.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	19

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

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES.

No se contempla esta opción.

5. Controles de Instalaciones, Gestión y Operación.

5.1. CONTROLES FÍSICOS.

Según lo definido en la DPC de Sello de Tiempo de Security Data.

5.2. CONTROLES DE PROCEDIMIENTO.

5.2.1. Roles de Confianza.

Los roles de confianza son los que se describen en las respectivas Declaración de Prácticas de Certificación, 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.

5.3. CONTROLES DE PERSONAL.

5.3.1. Calificaciones, Experiencia y Requisitos.

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

Security Data se asegura que los operadores de registro sean personas confiables para realizar las tareas de registro. Adicional los operadores de registro recibirán una inducción de preparación para la realización de las tareas de registro y validación de las peticiones. Al final de dicha inducción, procederá a evaluar sus conocimientos.

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. Comprobación de Antecedentes.

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

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	20

Security Data verifica periódicamente los antecedentes penales y policiales de los colaboradores, de acuerdo a lo definido en los procedimientos internos.

5.3.3. Requisitos de formación.

El personal de Security Data que administra los sistemas para la solicitud de emisión, revocación, modificación o suspensión, debe recibir una capacitación continua respecto:

- Certificados digitales.
- Firma electrónica.
- Regulaciones.
- Políticas de seguridad y privacidad.
- DPC y PC.
- Plan de contingencia.
- Funciones respecto de su rol.
- Seguridad de la Información.

5.3.4. Frecuencia y requisito de reentrenamiento.

La frecuencia de la capacitación deberá ser de al menos una vez antes de operar en Security Data y luego de manera anual.

5.3.5. Frecuencia y requisito de reentrenamiento.

No estipulado.

5.3.6. 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.

5.3.7. Requisitos del contratista independiente.

Los empleados contratados para realizar tareas confiables deberán firmar con anterioridad el acuerdo de confidencialidad, contrato y los requerimientos operacionales empleados por Security Data Seguridad en Datos y Firma Digital S.A.

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

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	21

5.3.8. Documentación suministrada al Personal.

Security Data pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las políticas y prácticas que rigen dichos procesos y la documentación de seguridad.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

5.4. PROCEDIMIENTOS DE REGISTRO DE AUDITORÍA.

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 AC. Estos incluyen los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de SECURITY DATA a través de la red.
- Intentos de accesos no autorizados a la red interna de de SECURITY DATA.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de SECURITY DATA.
- Encendido y apagado de la aplicación de SECURITY DATA.
- Cambios en los detalles de SECURITY DATA y/o sus claves.
- Cambios en la creación de perfiles de certificados.
- Generación de claves propias.
- Eventos del ciclo de vida del certificado.
- Eventos asociados al uso del módulo criptográfico de SECURITY DATA.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

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

- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal que realiza tareas de confianza en la AC.
- 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.
- Posesión de datos de activación, para operaciones con la clave privada de las AC.

5.4.2. Frecuencia de Procesado de Registros de Auditoría.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	22

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

Se 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.

Los registros o 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 Entidad 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 un centro de custodia externo de SECURITY DATA.

5.4.6. Sistema de Recolección de Información de Auditoría.

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

5.4.7. Notificación de Eventos.

SECURITY DATA establece que se toma en consideración la posibilidad de permitir la notificación a un titular en los casos en que se establezca que el evento es de índole accidental y resulta probable que pueda volver a ocurrir.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	23

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. ARCHIVO DE REGISTRO.

5.5.1. Tipo de Registros Archivados.

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

- Todos los datos de la auditoría
- Solicitudes de emisión y revocación de certificados
- Logs de 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

La CA es responsable del correcto archivo de todo este material y documentación.

5.5.2. Periodo de conservación de los datos.

Se 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.

5.5.3. Protección del Archivo.

La CA 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.

La CA 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.

La TSA 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.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	24

- 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.

5.6. CAMBIO DE CLAVE.

Según lo estipulado en la DPC de Sello de tiempo de Security Data.

5.7. COMPROMISO Y RECUPERACIÓN ANTE DESASTRES.

5.7.1. Procedimientos de Manejo de Incidentes y Compromisos.

El procedimiento se detalla en la DPC de Sello de Tiempo de Security Data.

5.7.2. Recursos Informáticos, 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 compromiso de Clave Privada de la entidad.

El procedimiento se detalla en la DPC de Sello de Tiempo de Security Data.

5.7.4. Capacidades de Continuidad de Negocio después de un Desastre.

Las acciones se detallan en la DPC de Sello de Tiempo de Security Data.

5.8. TERMINACIÓN O CESE.

Antes del cese de su actividad Security Data realizará las siguientes actuaciones:

- Protección de los registros de auditoría.
- Notificar a los suscriptores, titulares y terceros que confían sobre el cese de las operaciones con al menos treinta (30) días de anticipación.
- Informar a la ARCOTEL con al menos sesenta (60) días de anticipación.

Security Data toma medidas para transferir los registros de auditoría a la Autoridad Competente por el periodo de 10 años luego de generado el registro.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	25

Todas las solicitudes y contratos existentes de los suscriptores y titulares serán transferidos, a la Autoridad Competente o a otro PSC designado por éste, en cumplimiento de las garantías y responsabilidades previamente establecidas.

Se advertirá a todos los suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por una AC que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la página Web de Security Data.

6. Controles Técnicos de Seguridad.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.

El proceso de generación e instalación se realizará según lo definido en la DPC de sello de tiempo de Security Data.

La generación de la clave privada del certificado digital con el cual se firman los sellos de tiempo es realizada en un ambiente físico seguro (conforme a la sección 7.4.4 de la RFC 3628), por personal confiable (sección 7.4.3 de la RFC 3628) bajo, al menos, autorización de dos personas.

La generación de la clave privada se realiza en un módulo hardware de seguridad – HSM con certificaciones FIPS 140-2 nivel 3 o Common Criteria EAL 4+ y su administración es protegida por al menos dos personas.

6.2. PROTECCIÓN DE CLAVES PRIVADAS E INGENIERÍA DE MÓDULOS CRIPTOGRÁFICOS.

Los controles se estipulan según lo definido en la DPC de Sello de Tiempo de Security Data.

La clave privada del certificado de firma de cada sello de tiempo es resguardada durante su uso dentro de un módulo hardware criptográfico con certificación FIPS 140-2 nivel 3. Las copias de respaldo se almacenan en un módulo criptográfico del mismo nivel de seguridad.

6.3. OTROS ASPECTOS DE LA GESTIÓN DE PARES DE CLAVES.

Los controles se estipulan según lo definido en la DPC de Sello de Tiempo de Security Data.

6.4. DATOS DE ACTIVACIÓN.

Los controles se estipulan según lo definido en la DPC de Sello de Tiempo de Security Data.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA.

Los controles se estipulan según lo definido en la DPC de Sello de Tiempo de Security Data.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	26

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA.

Los controles se estipulan según lo definido en la DPC de Sello de Tiempo de Security Data.

6.7. CONTROLES DE SEGURIDAD DE LA RED.

Los controles se estipulan según lo definido en la DPC de Sello de Tiempo de Security Data.

6.8. SELLADO DE TIEMPO.

6.8.1. Tipos y Usos de los Sellos de Tiempo.

Los sellos de tiempo emitidos por la CA de Security Data cumplen lo siguiente:

- Los sellos de tiempo son conformes a la RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.
- El sello de tiempo incluye un identificador de la política de sello de tiempo, en concordancia con la TSA y la TSU de Security Data. (ver sección Validación de los sellos de tiempo).
- El sello de tiempo incluye el resumen de los datos firmados (HASH) incluido en la correspondiente petición de sello de tiempo.
- El sello de tiempo está firmado por una clave generada para este propósito, correspondiente a la TSU de la TSA Security Data.
- El algoritmo de hash de firma de los sellos de tiempo es SHA-256.
- Se utiliza un servicio de sincronización a la fuente de tiempo confiable.
- El tiempo incluido en el sello de tiempo está sincronizado con la hora UTC de la fuente de tiempo confiable dentro de la precisión de +/- 1 segundo, la cual se incluye en el sello de tiempo (el valor del campo accuracy en el sello de tiempo es 1 segundo).
- Si se detecta que el reloj del proveedor del sello de tiempo se encuentra fuera de la precisión indicada, los sellos de tiempo no se emiten.

Los clientes que reciben este servicio de sellado de tiempo están obligados a cumplir con lo dispuesto por la normativa vigente, a respetar lo indicado en los contratos firmados con esta Autoridad de Sellado, verificar la corrección de la firma del sello de tiempo, la validez del certificado de la TSU, así como verificar que el hash del sello de tiempo coincide con el que se envió.

6.8.2. Validación de los Sellos de Tiempo.

Los terceros deben comprobar el estado de los sellos de tiempo electrónicos en los cuales desean confiar, para ello deberán consultar el estado del Certificado de TSU. Un método por el cual se puede verificar el estado de los certificados de TSU es consultando la Lista de Revocación de Certificados más reciente emitida por Security Data como Autoridad de Certificación, responsable de la emisión de estos.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	27

Las Listas de Revocación de Certificados o CRL se publican en la página web de Security Data, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- Las CRL se las puede descargar de:
 - <http://crl1.securitydata.net.ec/subca2crl1/crlfile.crl>
 - <http://crl2.securitydata.net.ec/subca2crl2/crlfile.crl>

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

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

6.8.3. Exactitud de la Hora en el Sello de Tiempo.

El tiempo incluido en el sello de tiempo está sincronizado con la hora UTC de la fuente de tiempo confiable dentro de la precisión de +/- 1 segundo, la cual se incluye en el sello de tiempo (el valor del campo accuracy en el sello de tiempo es 1 segundo)

6.8.4. Límites de Uso del Certificado.

Los sellos de tiempo electrónico limitan su uso en las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios.

No se utilizarán los sellos de tiempo para fines distintos de los especificados anteriormente.

7. Perfiles de Certificados, CRL y OCSP.

7.1. PERFIL DEL CERTIFICADO.

Cada sello de tiempo emitido por SECURITY DATA S.A. contiene toda la documentación que requiere la normativa, como se muestra en la siguiente tabla:

Campo		Oblig.	Crit.	Observaciones OID 1.3.6.1.4.1.oid_AC.2.5.1
Cert. Sellado de Tiempo	Autenticación y Firma			
1. Basic structure				
1.1. Version	"2"	SI		El literal "2" corresponde a la versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	SI		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		SI		
1.3.1. Algorithm	SHA-256 with RSA Signature	SI		1.2.840.113549.1.1.11
1.4. Issuer		SI		

CÓDIGO	SD-ID-PE-12
VERSIÓN	V2
FECHA DE APROBACIÓN	13/02/2026
PÁGINAS	28

1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	SI		OID 2.5.4.6
1.4.3. Organization Name(O)	Nombre de la AC Subordinada "Organización"	SI		OID 2.5.4.10
1.4.5. Common Name (CN)	Nombre de la AC Subordinada	SI		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity	Se recomienda (máximo 5 años)	SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Country Name (C)	País donde se encuentra la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	SI		OID 2.5.4.6
1.6.2. Organization Name (O)	Nombre de la Persona Jurídica (Pública o Privada) Titular de la Firma solicitante del sello de tiempo ej. "NOTARIA"	SI		OID 2.5.4.10
1.6.3. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada), Ciudad) ej. QUITO	SI		OID 2.5.4.7
1.6.4. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) a la que esta vinculado el Sello de Tiempo "VAT(CÓDIGO_PAIS)-RUC Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.5. Serial Number	Número de Registro Unico de Contribuyente de la Persona Jurídica (Pública o Privada) Ej. "1716151413001"	SI		OID 2.5.4.5
1.6.6. Common Name (CN)	Nombre del Servicio "Sellado de tiempo de la Persona Jurídica (Publica o Privada)"	SI		OID 2.5.4.3
1.6.7. Organization Unit Name (OU)	Nombre de la Unidad Organizativa de la Persona Jurídica (Pública o Privada) Ej. UNIDAD DE SELLADO DE TIEMPO DE LA NOTARIA	SI		OID 2.5.4.11
1.7. Subject Public Key Info		SI		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico 2048 bits	SI		Acorde ETSITS 119312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es Obligatorio siempre y cuando la clave pública de la AC se distribuya en formato de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	SI		
2.3.2. Content commitment	No seleccionado. "0"			
2.3.3. Key Encipherment	No seleccionado. "0"			

CÓDIGO	SD-ID-PE-12
VERSIÓN	V2
FECHA DE APROBACIÓN	13/02/2026
PÁGINAS	29

2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		SI		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.5.1	SI		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		SI		
2.4.1.1.1 CPS URI	(https://www.repo_example.com/dpc/)	SI		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE SALLADO DE TIEMPO"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		SI	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la Entidad Acreditada "info@example.com.ec"	SI		
2.6. Extended Key Usage		SI	SI	OID 2.5.29.37 (Marcado como crítico según RFC 3161)
2.6.1. TimeStamping	Presente (1.3.6.1.5.5.7.3.8)	SI		
2.7. cRLDistributionPoint		SI	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	(http://crl1.example.com/example1subordinada.crl)	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	(http://crl2.example.com/example2subordinada.crl)	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		SI	NO	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		SI		
2.8.1.1. Access Method	id-ad-ocsp	SI		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	(http://ocsp1.example.com/ocsp/)	SI		URL de acceso al OCSP(http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	(http://ocsp2.example.com/ocsp/)	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		No es Obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	30

2.8.2.1.1 Access Location	(http://www.example.com/subordinate1.crt)	No		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		SI	SI	OID 2.5.29.19
2.9.1. cA	FALSE	SI		

7.1.1. Número de Versión.

Especificada en el Perfil del Certificado.

7.1.2. Extensiones del Certificado.

Especificado en el Perfil del Certificado.

7.1.3. Identificadores de Objetos de Algoritmos.

Especificado en el Perfil del Certificado.

7.1.4. Formas de los nombres.

Especificado en el Perfil del Certificado.

7.1.5. Restricciones de Nombre.

No se emplea la extensión X.509 “Name Constraints” en los certificados de esta política, es decir no se incluyen restricciones técnicas mediante el OID 2.5.29.30. En consecuencia, no existen “permittedSubtrees/excludedSubtrees” expresados en el certificado.

La limitación de nombres se realiza por perfil de emisión, plantilla de sujeto y campos permitidos, de modo que los certificados emitidos bajo esta política deben: Contener un Subject DN orientado a identificar el servicio de sellado de tiempo (TSA) que incluyen campos C, L, O, CN, OU, Serial Number y Organization Identifier..

7.1.6. Identificador de objeto de Política de Certificado.

El OID de la presente Política es 1.3.6.1.4.1.37746.102.2.5.1

7.1.7. Uso de la extensión Restricciones de Política.

No se utiliza la extensión X.509 “Policy Constraints” bajo el OID 2.5.29.36 en los certificados de esta política. Por lo tanto: No se aplican restricciones técnicas de “requireExplicitPolicy” ni “inhibitPolicyMapping” dentro del certificado final.

 <p>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	31

7.1.8. Sintaxis y Semántica de los calificadores de Política.

La CA declara las políticas aplicables en la extensión Certificate Policies con OID 2.5.29.32, la CA incluye Policy Qualifiers de los tipos:

- CPS URI con OID 1.3.6.1.5.5.7.2.1: enlace al documento PC vigente aplicable al servicio de TSA.
- User Notice con OID 1.3.6.1.5.5.7.2.2: texto corto que describe el tipo/alcance del certificado como "CERTIFICADO DE SELLADO DE TIEMPO"

Semántica:

- El CPS URI es informativo: apunta al documento normativo donde se describen controles, responsabilidades y límites del uso.
- El User Notice es informativo: resume el propósito del certificado y puede advertir sobre restricciones de uso.

7.1.9. Semántica de procesamiento para la Extensión de Políticas de Certificados Críticos.

En esta política, la extensión Certificate Policies con OID 2.5.29.32 se emite como NO crítica.

Las aplicaciones que validan la cadena deben procesar la extensión Certificate Policies cuando el caso de uso requiera verificar propósito/política.

7.2. PERFIL CRL.

El perfil de las CRL's se corresponde con el propuesto en las políticas de certificación correspondientes, y con el estándar X.509 de la 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Las CRL's son firmadas por la autoridad de certificación que ha emitido los certificados.

7.2.1. Número de Versión.

Las CRL emitidas por la AC son de la versión 2.

7.2.2. CRL y extensiones de entrada CRL.

Las CRL y extensiones se encuentran definidas en las DPC de Security Data.

7.3. PERFIL OCSP.

Los certificados emitidos para el servicio de validación OCSP siguen un perfil de certificado X.509 v3 destinado exclusivamente a firma de respuestas OCSP. El certificado NO actúa como CA donde CA=FALSE y su uso se restringe por EKU al propósito OCSPSigning.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	32

Elementos característicos del perfil:

- Subject DN identifica al Respondedor OCSP
- Basic Constraints: CA=FALSE.
- EKU: OCSPSigning con OID 1.3.6.1.5.5.7.3.9
- Contiene la extensión OCSP No Check para permitir que las partes confiantes no requieran verificación de revocación adicional de este certificado durante la validación OCSP.
- Publica puntos de CRL Distribution Points y Authority Information Access para obtención de cadena y emisor.

7.3.1. Número de Versión.

El certificado OCSP se emite como X.509 Versión 3, para permitir el uso de extensiones críticas y no críticas necesarias para operación del servicio OCSP.

7.3.2. Extensiones OCSP.

A continuación, se especifican las extensiones presentes en el certificado OCSP y su semántica de uso dentro de este perfil:

- Extensiones críticas
 - Key Usage con OID 2.5.29.15 – CRÍTICA
 - digitalSignature = TRUE firma de respuestas OCSP.
 - contentCommitment / nonRepudiation = TRUE
 - El resto de bits de KeyUsage se mantienen en FALSE, no se permite cifrado, firma de certificados, ni firma de CRL.
 - Basic Constraints con OID 2.5.29.19 – CRÍTICA
 - CA = FALSE.
 - Sin pathLenConstraint.
 - Confirma que el certificado es de entidad final y no puede emitir certificados.
- Extensiones no críticas
 - Extended Key Usage con OID 2.5.29.37 – NO CRÍTICA
 - Incluye id-kp-OCSPSigning con OID 1.3.6.1.5.5.7.3.9.
 - Restringe el uso del certificado a la firma de respuestas OCSP.
 - OCSP No Check con OID 1.3.6.1.5.5.7.48.1.5 – NO CRÍTICA
 - Indica que las partes confiantes pueden omitir la comprobación de revocación vía CRL/OCSP de este certificado OCSP al validar respuestas OCSP, según prácticas habituales para certificados de respondedores OCSP.
 - Certificate Policies con OID 2.5.29.32 – NO CRÍTICA
 - Incluye el OID de política aplicable al certificado OCSP: 1.3.6.1.4.1.37746.2.6.1
 - Además, se publica la referencia documental de política:

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	33

- DPC:
 - <https://www.securitydata.net.ec/normativas/dpcocsp.pdf>
- User Notice: "CERTIFICADO DE VALIDACION OCSP"
- Subject Alternative Name con OID 2.5.29.17 – NO CRÍTICA
 - Incluye rfc822Name con correo de contacto del servicio:
- CRL Distribution Points con OID 2.5.29.31 – NO CRÍTICA
 - Publica puntos de distribución de CRL del emisor
- Authority Information Access con OID 1.3.6.1.5.5.7.1.1 – NO CRÍTICA
 - Publica calssuers para descarga del certificado emisor (URL HTTP del emisor).
- Subject Key Identifier con OID 2.5.29.14 – NO CRÍTICA
 - Identificador de clave del sujeto para facilitar construcción y validación de cadena.
- Authority Key Identifier con OID 2.5.29.35 – NO CRÍTICA
 - Identificador de clave de la CA emisora para facilitar construcción y validación de cadena.

8. Auditorías de cumplimiento y otros controles.

El sistema de expedición de Certificados de SECURITY DATA es sometido a auditorías para mantener activo el Sello Webtrust.

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 a la TSA de la jerarquía para garantizar en todo momento su adecuación a los requerimientos marcados por las políticas de certificación de la jerarquía.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	34

8.4. ASPECTOS CUBIERTOS POR LOS CONTROLES.

La auditoría verifica los siguientes principios:

- a) **Publicación de la Información:** Que la CA hace públicas las Prácticas de Negocio y de Gestión de Certificados en la DPC, así como la política de privacidad de la información y protección de datos personales y proporciona sus servicios en conformidad con dichas afirmaciones.
- b) **Integridad de Servicio:** Que la CA mantiene controles efectivos para asegurar razonablemente que:
 - La información del suscriptor es autenticada adecuadamente (para las actividades de registro realizadas por la CA), y
- c) **Controles generales.** Que la CA 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 CA 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 la CA son adecuadamente autorizadas y realizadas para mantener la integridad de los mismos.

8.5. ACCIONES ADOPTADAS COMO RESULTADO.

Las deficiencias detectadas durante el proceso de Auditoría deben ser subsanadas a través de un Plan de Acciones correctivas que contenga las acciones, procedimientos o implementación de los controles requeridos para minimizar riesgos.

En caso de que sean detectadas incidencias o no-conformidades, se tomarán las medidas oportunas para su resolución en el menor tiempo posible, según los procedimientos establecidos por Security Data.

8.6. COMUNICACIÓN DE RESULTADOS.

El auditor comunicará los resultados a la Alta Dirección, y de ser necesario, a los dueños de cada proceso, en el caso de requerirse el análisis y la resolución de cualquier desvío de cumplimiento, Security Data será encargado de levantar un plan de acción correctiva posterior.

9. Otros Asuntos Comerciales y Legales.

9.1. TARIFAS.

 <p>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<p>POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO</p>	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	35

9.1.1. Tarifas de Emisión o Renovación de certificados.

Las tarifas de emisión se encuentran estipuladas en la DPC de Sello de Tiempo de Security Data.

9.1.2. Tarifas de acceso al certificado.

Las tarifas de acceso se encuentran estipuladas en la DPC de Sello de Tiempo de Security Data.

9.1.3. Tarifas de Acceso a la Información de revocación o estado.

Las tarifas de acceso se encuentran estipuladas en la DPC de Sello de Tiempo de Security Data.

9.1.4. Tarifa por Otros Servicios.

Las tarifas se encuentran estipuladas en la DPC de Sello de Tiempo de Security Data.

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 info@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. RESPONSABILIDAD FINANCIERA.

9.2.1. Cobertura del Seguro.

El seguro cubre todos los perjuicios contractuales y extracontractuales de los titulares clientes de SECURITY DATA, que confían exenta de culpa 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

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	36

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 la SECURITY DATA en el desarrollo de las actividades para las cuales cuenta con autorización.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN EMPRESARIAL.

El personal de Security Data deberá firmar contratos que incluyen cláusulas de confidencialidad respecto de la protección de la privacidad y confidencialidad de toda la información presentada por los clientes, así como también un acuerdo de confidencialidad. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados, podrá dar lugar al cese del contrato laboral.

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 AC mantendrá como información no privada la siguiente:

- La contenida en la presente PC y DPC.
- Toda la información contenida en los certificados emitidos y listas de revocación de 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.
- Toda la información clasificada expresamente como "PÚBLICA".
- Información en relación a la revocación de un certificado.
- Cualquier otra información cuya publicidad sea impuesta normativamente

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	37

9.3.3. Deber 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 la normativa vigente, en los términos y condiciones publicados. En lo que se refiere a protección de datos personales, se aplicará la normativa aplicable en esta materia, en especial la Ley Orgánica de Protección de Datos Personales (LOPDP), su reglamento y demás disposiciones emitidas por la autoridad competente.

Asimismo, Security Data implementará medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos personales tratados.

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.

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.

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

Los datos de carácter personal no podrán ser comunicados a terceros, sin la debida notificación y consentimiento de su dueño.

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

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	38

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 se estipula

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 la CA.

Se garantiza, que cumple con la totalidad de los requisitos establecidos en la Política de Certificación, Declaración de Prácticas de Certificación, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento.

Security Data presta los servicios de Certificación Digital conforme con esta Política de certificación, Declaración de Prácticas de Certificación de Sellado de Tiempo y a los estándares de aplicación. Asimismo, emite los sellos de tiempo según la información que obra en su poder y libres de errores de entrada de datos entregando los servicios con la confiabilidad y exactitud establecida en los respectivos contratos y en el presente documento. Se brindará el servicio de sello de tiempo como servicio bien con el certificado de TSA emitido para la AC o con un TSA emitido para el cliente y regido en la norma técnica.

Security Data informa al suscriptor de los términos y condiciones relativos al uso del sello, de su precio y de sus limitaciones de uso.

Security Data vincula a suscriptores, poseedores de claves y terceros que confían en certificados, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en el presente documento.
- Límites de uso de los sellos de tiempo.
- Información sobre cómo validar un sello de tiempo, incluyendo el requisito de comprobar el estado de este, y las condiciones en las cuales se puede confiar razonablemente en él, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.

9.6.2. Declaraciones y Garantías de la RA.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	39

Las responsabilidades de la entidad de registro son las siguientes:

- Verificar la identidad de los solicitantes de certificados, así como también la veracidad de la información y documentos suministrados.
- Respetar lo dispuesto en la DPC y PC.
- Proporcionar la información mínima necesaria para el uso de los certificados al solicitante, cuya información deberá transmitirse de forma gratuita, por escrito o por vía electrónica.
- Tomar medidas contra la falsificación de certificados y garantizar la confidencialidad de los datos de creación de firma durante el proceso de generación, así como su entrega por un procedimiento seguro al suscriptor.
- No copiar ni almacenar los datos de creación de firma del suscriptor.
- Proteger los datos personales de los solicitantes y usuarios de certificados digitales o electrónicos.

9.6.3. Declaraciones y Garantías de los Suscriptores.

El Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- Integrar, configurar y utilizar el servicio de estampado cronológico de la AC, conforme a las instrucciones enviadas por la AC al Solicitante.
- Utilizar sistemas cliente que envíen peticiones al servicio de estampado cronológico de la AC e interpreten sus respuestas conforme al formato establecido en la RFC 3161, y que realicen las verificaciones del estado del certificado de la TSA.
- Respetar lo dispuesto en los instrumentos jurídicos vinculantes con la AC.
- El Suscriptor será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta PC.

9.6.4. Declaraciones y Garantías de la parte que Confía.

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y también:

- a) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los sellos de tiempo en los que confían, y aceptar sujetarse a los mismos.
- b) Notificar a Security Data cualquier situación irregular con respecto al servicio prestado por la AC.

La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC y esta PC.

El tercero que confía se obliga a no utilizar ningún tipo de información de estado de los sellos de tiempo o de ningún otro tipo que haya sido suministrada por Security Data, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	40

El tercero que confía se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de Ecuador, sin previo consentimiento escrito.

Adicionalmente, el tercero que confía se obliga a no comprometer intencionadamente la seguridad de los servicios de sellado de tiempo de Security Data.

Los servicios de sellado de tiempo prestados por Security Data no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

9.6.5. Declaraciones y Garantías de Otros Participantes.

Sin estipulación.

9.7. RENUNCIAS A GARANTÍAS.

SECURITY DATA por la presente renuncia a todas las garantías, incluida la garantía de comerciabilidad y / o idoneidad para un propósito particular que no sea en la medida prohibida por la ley o expresamente estipulada en esta PC y DPC.

9.8. LIMITACIONES DE RESPONSABILIDAD.

En la medida en que la CA de SECURITY DATA, haya emitido y administrado el certificado de sellado de tiempo de acuerdo con la PC / 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.

La TSA de SECURITY DATA será responsable ante los titulares de certificados o los terceros que confían por pérdidas directas derivadas de cualquier incumplimiento de esta PC y DPC o por cualquier otra responsabilidad en la que puedan incurrir en un contrato, agravio u otro, incluida la responsabilidad por negligencia por suscriptor o tercero de confianza o tercero por certificado, siempre que el suscriptor, el tercero de confianza o el tercero cumplan plenamente con dicho PC y DPC.

La responsabilidad de la TSA de SECURITY DATA, a cualquier persona por daños que surjan bajo, fuera o relacionado con esta PC y DPC, Acuerdo de Suscriptor, contrato aplicable o cualquier otro acuerdo relacionado, ya sea por contrato, garantía, agravio o de otro modo, se limitará a los daños reales sufridos por esa persona. La TSA de SECURITY DATA no será responsable por daños indirectos, consecuentes, incidentales, especiales, ejemplares o punitivos con respecto a cualquier persona, independientemente de cómo dichos daños o responsabilidad puede surgir, ya sea en agravio, negligencia, equidad, contrato, estatuto, derecho consuetudinario o de otra manera.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	41

9.9. INDEMNIZACIONES.

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

9.10. PLAZO Y TERMINACIÓN.

9.10.1. Plazo.

Este documento de Política de Certificación 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 más nueva.

9.10.2. Terminación.

Este documento de Política de Certificación y DPC, y cualquier enmienda permanecerán en vigor hasta que se modifique o reemplace por una versión más nueva.

9.11. AVISOS Y COMUNICACIONES INDIVIDUALES CON LOS PARTICIPANTES.

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 enmendaduras 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.

9.13. DISPOSICIONES DE RESOLUCIÓN DE DISPUTAS.

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

9.14. 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, Norma Técnica para la Prestación de Servicios de Certificación y Servicios Relacionados, emitida por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

9.15. CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE.

	POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	42

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. DISPOSICIONES DIVERSAS.

9.16.1. Acuerdo Completo.

Sin estipulación.

9.16.2. Cesión.

Las CA emisoras, los suscriptores, los terceros que confían, las Entidades de registro o cualquier otra entidad que opere bajo esta Política de Certificación y no tienen derecho a asignar ninguno de sus derechos u obligaciones bajo este documento sin el consentimiento previo por escrito de SECURITY DATA.

9.16.3. Divisibilidad.

Si alguna de las disposiciones de esta Política de Certificación y Declaración de Prácticas 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.

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

9.17. OTRAS DISPOSICIONES.

Sin estipulación.

10. Control de Aprobaciones.

 <p>SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<p>POLÍTICA DE CERTIFICACIÓN DE SELLO DE TIEMPO</p>	CÓDIGO	SD-ID-PE-12
		VERSIÓN	V2
		FECHA DE APROBACIÓN	13/02/2026
		PÁGINAS	43

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