

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



POLÍTICA DE
CERTIFICACIÓN DE SELLO
ELECTRÓNICO

febrero 12

2026

 <p>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<p>POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO</p>	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	2

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	FECHA	ELABORADO POR	REVISADO POR	APROBADO POR
V1	Edición Inicial	22/12/2025	Supervisor Legal	Chief Technology Officer (CTO)	Gerente General
V2	Actualización general de la PC conforme a la Normativa Técnica y RFC 3647.	12/02/2026	Coordinador del Sistema de Gestión	Chief Technology Officer (CTO) Supervisor Legal	Gerente General

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		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.	Suscriptores.....	10
1.3.4.	Partes que Confían.	10
1.3.5.	Certificado de Sello Electrónico.	10
1.4.	USO DEL CERTIFICADO.	11
1.4.1.	Usos apropiados del Certificado.	11
1.4.2.	Usos No Autorizados 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.	12
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.	PROCEDIMIENTO DE APROBACIÓN.....	14
2.3.	TIEMPO O FRECUENCIA DE PUBLICACIÓN.	14
2.4.	CONTROLES DE ACCESO A LOS REPOSITORIOS.	14
3.	Identificación y Autenticación.....	15
3.1.	DENOMINACIÓN.	15
3.1.1.	Tipos de Nombres.	15
3.1.2.	Necesidad de que los nombres sean significativos.....	15
3.1.3.	Seudónimos.....	15
3.1.4.	Reglas para interpretar de que los nombres sean significativos.	15

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

3.1.5.	Singularidad de los Nombres.	16
3.1.6.	Reconocimiento, autenticación y función de las marcas.	16
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 una Organización (Persona Jurídica).	16
3.2.3.	Autenticación de la Identidad Individual.	17
3.2.4.	Información de Titular No Verificada.	17
3.2.5.	Validación de la Autoridad.	17
3.2.6.	Criterios de Interoperabilidad.	17
3.3.	IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN DE CLAVES.	18
3.3.1.	Identificación y Autenticación para la renovación rutinaria de claves.	18
3.3.2.	Identificación y Autenticación para la renovación de claves después de la revocación.	18
3.4.	IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA SOLICITUD DE REVOCACIÓN.	18
4.	Requisitos Operacionales para el Ciclo de Vida de los Certificados.	18
4.1.	SOLICITUD DE CERTIFICADOS.	18
4.1.1.	Quién puede solicitar un Certificado.	18
4.1.2.	Procesos de Solicitud de Certificados.	18
4.1.3.	Validez del Certificado de Sello Electrónico.	19
4.2.	PROCEDIMIENTO DE TRAMITACIÓN.	19
4.2.1.	Realización de funciones de Identificación y Autenticación.	19
4.2.2.	Aprobación o rechazo de la solicitud de certificados.	19
4.2.3.	Tiempo de tramitación de las solicitudes de Certificados.	20
4.3.	EMISIÓN DEL CERTIFICADO.	20
4.3.1.	Acciones de la AC durante la Emisión de los Certificados.	20
4.3.2.	Entrega del Certificado.	20
4.4.	ACEPTACIÓN DEL CERTIFICADO.	20
4.4.1.	Forma en la que se Acepta el Certificado.	20
4.4.2.	Publicación del Certificado.	20
4.4.3.	Notificación de la Emisión del Certificado por la AC a terceros.	21
4.5.	USO DE PARES DE CLAVES Y CERTIFICADOS.	21
4.5.1.	Uso de la Clave Privada y del Certificado del Suscriptor.	21

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

4.5.2.	Uso de Clave Pública y Certificado de la parte que confía.....	21
4.6.	RENOVACIÓN DE CERTIFICADOS.....	21
4.7.	CAMBIO DE CLAVE DEL CERTIFICADO.....	21
4.7.1.	Circunstancias para la Renovación del Certificado.....	21
4.7.2.	Personas autorizadas para solicitar renovación.....	21
4.7.3.	Aprobación o rechazo de las solicitudes de renovación.....	22
4.7.4.	Notificación de la Renovación del Certificado.....	22
4.7.5.	Aceptación de la Renovación del Certificado.....	22
4.7.6.	Publicación del Certificado Renovado.....	22
4.7.7.	Notificación de la emisión de Certificados a otras entidades.....	22
4.8.	MODIFICACIÓN DE CERTIFICADOS.....	22
4.9.	REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	22
4.10.	SERVICIOS DE ESTADO DE CERTIFICADOS.....	22
4.10.1.	Características Operativas.....	22
4.10.2.	Disponibilidad del Servicio.....	23
4.10.3.	Características Opcionales.....	23
4.11.	FIN DE LA SUSCRIPCIÓN.....	23
4.12.	CUSTODIA Y RECUPERACIÓN DE CLAVES.....	23
5.	Controles de Instalaciones, Gestión y Operación.....	23
5.1.	CONTROLES DE SEGURIDAD FÍSICA.....	24
5.2.	CONTROLES DE PROCEDIMIENTO.....	24
5.3.	CONTROLES DE PERSONAL.....	24
5.4.	PROCEDIMIENTO DE REGISTRO DE AUDITORÍA.....	24
5.4.1.	Tipos de Eventos Registrados.....	24
5.4.2.	Frecuencia de Procesado de Registros de Auditoría.....	25
5.4.3.	Periodo de Conservación de los Registros de Auditoría.....	25
5.4.4.	Protección de los Registros.....	25
5.4.5.	Procedimientos de Respaldo de los Registros de Auditoría.....	25
5.4.6.	Sistema de Recolección de Información de Auditoría.....	26
5.4.7.	Notificación de Eventos.....	26
5.4.8.	Análisis de Vulnerabilidades.....	26
5.5.	ARCHIVOS DE REGISTRO.....	26
5.6.	CAMBIO DE CLAVE.....	26

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

5.7.	COMPROMISO Y RECUPERACIÓN ANTE DESASTRES.....	26
5.8.	TERMINACIÓN DE CA.	26
6.	Controles Técnicos de Seguridad.	27
6.1.	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.	27
6.2.	PROTECCIÓN DE CLAVES PRIVADAS E INGENIERÍA DE MÓDULOS CRIPTOGRÁFICOS.	27
6.3.	OTROS ASPECTOS DE LA GESTIÓN DE PARES DE CLAVES.....	27
6.4.	DATOS DE ACTIVACIÓN.	27
6.5.	CONTROLES DE SEGURIDAD INFORMÁTICA.....	27
6.6.	CONTROLES TÉCNICOS DEL CICLO DE VIDA.	27
6.7.	CONTROLES DE SEGURIDAD DE LA RED.	27
6.8.	SELLADO DE TIEMPO.	28
7.	Perfiles de Certificados, CRL y OCSP.	28
7.1.	PERFIL DEL CERTIFICADO.....	28
7.1.1.	Número de Versión.	34
7.1.2.	Extensiones del Certificado.	34
7.1.3.	Identificadores de Objetos de Algoritmos.	34
7.1.4.	Formas de los nombres.	34
7.1.5.	Restricciones de Nombre.	34
7.1.6.	Identificador de objeto de Política de Certificado.	34
7.1.7.	Uso de la extensión Restricciones de Política.	34
7.1.8.	Sintaxis y Semántica de los calificadores de Política.....	35
7.1.9.	Semántica de procesamiento para la Extensión de Políticas de Certificados Críticos.	35
7.2.	PERFIL CRL.	35
7.2.1.	Número de Versión.	36
7.2.2.	CRL y extensiones de entrada CRL.	36
7.3.	PERFIL OCSP.	36
7.3.1.	Número de Versión.	36
7.3.2.	Extensiones OCSP.....	36
8.	Auditorías de cumplimiento y otros controles.....	37
8.1.	FRECUENCIA DE LAS AUDITORIAS.	37
8.2.	CUALIFICACIÓN DEL AUDITOR.	38
8.3.	RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA.....	38

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

8.4.	ASPECTOS CUBIERTOS POR LOS CONTROLES.....	38
8.5.	ACCIONES ADOPTADAS COMO RESULTADO.....	38
8.6.	COMUNICACIÓN DE RESULTADOS.	39
9.	Otros Asuntos Comerciales y Legales.....	39
9.1.	TARIFAS.	39
9.1.1.	Tarifas de Emisión o Renovación de certificados.....	39
9.1.2.	Tarifas de acceso al certificado.	39
9.1.3.	Tarifas de Acceso a la Información de revocación o estado.	39
9.1.4.	Tarifa por Otros Servicios.....	39
9.1.5.	Política de Reembolso.....	39
9.2.	RESPONSABILIDAD FINANCIERA.....	40
9.2.1.	Cobertura del Seguro.	40
9.2.2.	Otros Bienes.	40
9.2.3.	Seguro o Garantía de Cobertura para las Entidades Finales.....	40
9.3.	CONFIDENCIALIDAD DE LA INFORMACIÓN EMPRESARIAL.....	40
9.3.1.	Alcance de la Información Confidencial.....	41
9.3.2.	Información No Confidencial.....	41
9.3.3.	Deber de Proteger la Información Confidencial.....	41
9.4.	PRIVACIDAD DE LA INFORMACIÓN PERSONAL.....	41
9.4.1.	Política de Privacidad.	41
9.4.2.	Información tratada como Privada.	42
9.4.3.	Información No Calificada como Privada.....	42
9.4.4.	Responsabilidad de la Protección de los Datos de Carácter Personal.	42
9.4.5.	Notificación y Consentimiento para usar Datos de Carácter Personal.....	42
9.4.6.	Revelación en el marco de un proceso administrativo o judicial.....	42
9.4.7.	Otras circunstancias de revelación de información.	42
9.5.	DERECHOS DE PROPIEDAD INTELECTUAL.....	42
9.6.	DECLARACIONES Y GARANTÍAS.....	43
9.6.1.	Declaraciones y Garantías de la CA.....	43
9.6.2.	Declaraciones y Garantías de la RA.....	43
9.6.3.	Declaraciones y Garantías de los Suscriptores.....	44
9.6.4.	Declaraciones y Garantías de la parte que Confía.	44
9.6.5.	Declaraciones y Garantías de Otros Participantes.....	45

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

9.7.	RENUNCIAS A GARANTÍAS.....	45
9.8.	LIMITACIONES DE RESPONSABILIDAD.....	45
9.9.	INDEMNIZACIONES.	45
9.10.	PLAZO Y TERMINACIÓN.....	45
9.10.1.	Plazo.....	45
9.10.2.	Terminación.....	46
9.11.	AVISOS Y COMUNICACIONES INDIVIDUALES CON LOS PARTICIPANTES.....	46
9.12.	ENMIENDAS.....	46
9.13.	DISPOSICIONES DE RESOLUCIÓN DE DISPUTAS.	46
9.14.	LEY APLICABLE.....	46
9.15.	CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE.....	46
9.16.	DISPOSICIONES DIVERSAS.	46
9.16.1.	Acuerdo Completo.	46
9.16.2.	Cesión.....	47
9.16.3.	Divisibilidad.	47
9.16.4.	Ejecución.	47
9.16.5.	Fuerza Mayor.	47
9.17.	OTRAS DISPOSICIONES.....	47
10.	Control de Aprobaciones.....	48

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		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. (en adelante 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.

El presente documento es la Política de Certificación (PC) correspondiente a los certificados emitidos por Security Data del tipo “Sello Electrónico Archivo” y “Sello Electrónico DSCF”. Estos certificados pueden ser expedidos con la consideración de cualificados de acuerdo con lo establecido en la Norma Técnica para la Prestación de Servicios de Certificación y Servicios Relacionados, emitida por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y con la consideración de cualificados según lo definido en la legislación vigente.

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 emisión de Sello Electrónico, 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 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 Electrónico
Código del documento:	SD-ID-PE-13
Versión:	2
Descripción:	Política de Certificación de Sello Electrónico de Security Data Seguridad en Datos y Firma Digital S.A.
Fecha de publicación:	12 de febrero del 2026
Tipo de documento:	Público
OID:	OID de archivo: 1.3.6.1.4.1.37746.2.4.1 OID de DSCF: 1.3.6.1.4.1.37746.2.4.2

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		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. Suscriptores.

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

1.3.4. Partes que Confían.

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

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

1.3.5. Certificado de Sello Electrónico.

Se trata de un certificado para persona jurídica, que suscribe los términos y condiciones de uso de un certificado, y cuya identidad queda vinculada a los Datos de Verificación de sello (Clave Pública) del certificado emitido por Security Data. Por lo tanto, la identidad del suscriptor del certificado queda vinculada a lo sellado electrónicamente por el creador de sello, utilizando los Datos de Creación de Sello (Clave Privada) asociados al certificado emitido por Security Data.

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	11

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 Security Data.

Se considerará que se hace un uso indebido de un certificado cuando éste sea utilizado para realizar operaciones no autorizadas según las Políticas de Certificados aplicables a cada uno de los certificados, 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 No Autorizados 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 demás documentos normativos.

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

1.5.2. Persona de Contacto.

Nombre:	SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.
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 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.

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.

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

Sello electrónico: Conjunto de datos en formato electrónico, creado mediante medios criptográficos seguros y asociado a un certificado de sello electrónico, que permite identificar a la entidad emisora y garantizar la integridad y autenticidad de los datos electrónicos a los que se aplica.

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.

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 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
OCSF:	Online Certificate Status Protocol.
PKI:	Infraestructura de Clave Pública (Public Key Infrastructure)
PSC:	Prestador de Servicios de Certificación
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)

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

SN: Apellido (SurName)
 ISO: International Organization for Standardization
 PKCS: Public Key Cryptography Standards, Estándares PKI
 UTF8: Único de Transformation Format – 8 bits.

2. Responsabilidades de Publicación y Repositorio.

2.1. REPOSITORIOS.

Declaración de Prácticas de Certificación: https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/declaracion.pdf

Política de Certificación: <https://www.securitydata.net.ec/normativas/pcselloelectronico.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. PROCEDIMIENTO DE APROBACIÓN.

La publicación de las revisiones de esta PC de Sello Electrónico 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 Sello Electrónico será revisada y si procede, actualizadas, anualmente o cuando se presente algún cambio.

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.

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

3. Identificación y Autenticación.

3.1. DENOMINACIÓN.

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 sean significativos.

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.

No se permitirá el uso de alias, seudónimos o denominaciones informales, abreviaturas que no consten en documentos oficiales, nombres comerciales no registrados, expresiones que puedan inducir a error, confusión o suplantación de identidad.

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

3.1.3. Seudónimos.

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

3.1.4. Reglas para interpretar de que los nombres sean significativos.

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 electrónico, sin ambigüedades ni elementos que puedan inducir a error respecto de su identidad, naturaleza jurídica o ámbito de actuación.

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	16

3.1.5. Singularidad 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.

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.

3.2.1. Método para Demostrar la Posesión de la Clave Privada.

Cuando se expide un certificado en un dispositivo hardware, la clave privada se crea en el instante previo a la generación del certificado, mediante un procedimiento que garantiza su confidencialidad y su vinculación con la identidad del solicitante.

Las claves se entregan al responsable a través de ficheros protegidos utilizando el estándar PKCS#12. La seguridad del proceso queda garantizada debido a que el código de acceso al fichero PKCS#12 que posibilita la instalación de éste en las aplicaciones, es definido por el suscriptor y solo él tiene pleno conocimiento de la misma.

3.2.2. Autenticación de la Identidad de una Organización (Persona Jurídica).

Security Data deberá verificar los siguientes datos para poder autenticar la identidad de la organización:

- Los datos relativos a la denominación o razón social de la organización.
- Los datos relativos a la constitución, y personalidad jurídica del suscriptor.
- Los datos relativos a la extensión y vigencia de las facultades de representación del solicitante.
- Los datos relativos al registro único de contribuyentes de la organización RUC.

Además, el representante legal o miembro de empresa de la persona jurídica deberá presentar la cédula de identidad, pasaporte u otro medio reconocido en derecho que le identifique o se realizará un proceso de validación biométrica u otro medio reconocido en derecho que lo identifique.

Security Data Seguridad en Datos y Firma Digital se reserva el derecho de no emitir el certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

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

3.2.3. Autenticación de la Identidad Individual.

No aplicable para personas naturales.

3.2.4. Información de Titular 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.

Para certificados asociados a cargos institucionales, la AC comprueba que el solicitante esté debidamente autorizado por la organización correspondiente, mediante documentación formal que respalde dicha atribución, tales como designaciones, resoluciones internas o cartas de autorización emitidas por la autoridad competente.

La validación de la autoridad se realiza previo a la emisión del certificado, sobre la base de documentos oficiales y fuentes confiables, de conformidad con los procedimientos establecidos en la Declaración de Prácticas de Certificación.

La AC no asume responsabilidad por la validez posterior de la representación o autorización, una vez emitido el certificado, salvo en los casos previstos por la normativa vigente.

3.2.6. Criterios de Interoperabilidad.

Security Data emite certificados de sello electrónico conforme a estándares técnicos internacionalmente reconocidos, garantizando su interoperabilidad y posibilidad de validación por parte de sistemas, aplicaciones y terceros que confían.

Security Data se reserva el derecho de proporcionar servicios de interoperación e interoperar con otras AC; los términos y criterios de los cuales deben establecerse contractualmente.

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

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

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

Para los certificados de sello electrónico no se realizan renovaciones, sino que se realizan nuevas emisiones de certificados.

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

Los certificados de sellos electrónicos una vez que un certificado han sido revocados, no se puede renovar, y en su lugar se debe realizar una nueva emisión del certificado.

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:

- a) El propio suscriptor, identificándose y autenticándose en la página web en la Administración de la cuenta o de forma presencial, en las oficinas de Security Data Seguridad en Datos y Firma Digital.
- b) Cualquier Tercero Vinculado de Security Data Seguridad en Datos y Firma Digital: deberá identificar al suscriptor ante una petición de revocación según los propios medios que considere necesarios.

4. Requisitos Operacionales para el Ciclo de Vida de los Certificados.

4.1. SOLICITUD DE CERTIFICADOS.

4.1.1. Quién puede solicitar un Certificado.

Security Data solo admite solicitud de emisión de certificado tramitada por una persona natural bajo relación de dependencia, mayor de edad, con plena capacidad legal de obrar.

4.1.2. Procesos de Solicitud de Certificados.

El solicitante deberá acercarse a las oficinas de Security Data Seguridad en Datos y Firma Digital, teniendo en su poder la documentación requerida para gestionar la solicitud del certificado, en cuya presencia procederá a firmar el formulario de solicitud que deberá estar debidamente cumplimentado.

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

El solicitante o suscriptor es responsable de proporcionar información veraz y actualizada, así como de custodiar adecuadamente sus credenciales y utilizar el certificado conforme a lo establecido en la presente PC y DPC. La AC es responsable de gestionar el proceso de inscripción de manera segura, confiable y conforme a los estándares técnicos y regulatorios aplicables.

4.1.3. Validez del Certificado de Sello Electrónico.

La duración del certificado de sello electrónico se establecerá contractualmente entre el titular del sello electrónico y Security Data.

4.2. PROCEDIMIENTO DE TRAMITACIÓN.

4.2.1. Realización de funciones de Identificación y Autenticación.

El suscriptor deberá acreditar su identidad y presentar, en vigor, original o copia auténtica de la siguiente documentación:

- a) Dirección física y otros datos que permitan contactar con Él, para lo cual se solicitará el RUC.
- b) La AC, como acreditación del acto presencial y con el fin de imposibilitar el repudio del trámite realizado, podrá obtener un conjunto de evidencias biométricas: fotografía y/o video de validación.
- c) Cédula de identidad o pasaporte en caso de ciudadanos extranjeros, cuya fotografía permita cotejar la identidad de la persona compareciente.
- d) El Representante deberá disponer de poder suficiente de representación, haciendo entrega de documentos como: nombramiento, poder, nombramiento inscrito ante el ente regulador, y demás documentos habilitantes que Security Data considere necesarios.

Para autenticar a un Responsable de Certificado, se seguirá el mismo procedimiento que el especificado en el apartado anterior con la particularidad de que, en este supuesto, el poder de representación requerido al suscriptor será sustituido por la firma de una carta de Autorización. La carta deberá ser firmada por el Representante Legal.

4.2.2. Aprobación o rechazo de la solicitud de certificados.

Una vez realizada la solicitud del certificado, el Operador de Registro deberá verificar la información proporcionada por el solicitante, incluyendo la validación de la identidad del suscriptor.

Tras obtener las evidencias para comprobar la identidad, el operador de registro, revisará el proceso de identificación y comprobará las evidencias para aceptar o rechazar la validez del proceso de identificación, de conformidad con la normativa aplicable sobre las causas de rechazo de la video identificación.

En el proceso de validación intervendrán dando soporte el Departamento Legal y el Departamento Técnico, que revisará y validará técnicamente el certificado de petición.

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

Si la información no es correcta, el operador de registro denegará la petición, y se le comunicará al solicitante el motivo.

Si es correcta, se procederá con la atención, el pago o confirmación del pago del certificado y la firma del instrumento jurídico vinculante entre el suscriptor y/o el solicitante y Security Data Seguridad en Datos y Firma Digital. Se procederá entonces a la emisión del certificado.

4.2.3. Tiempo de tramitación de las solicitudes de Certificados.

La emisión de un certificado implica la aprobación final y completa de una solicitud por parte de Security Data. La emisión del certificado debe realizarse en un plazo máximo de 48 horas, una vez realizada la solicitud según lo definido en la DPC de Security Data.

4.3. EMISIÓN DEL CERTIFICADO.

La emisión del certificado se realizará según lo definido en la DPC de Security Data.

4.3.1. Acciones de la AC durante la Emisión de los Certificados.

Según lo definido en la DPC de Security Data.

4.3.2. Entrega del Certificado.

Según lo definido en la DPC de Security Data.

4.4. ACEPTACIÓN DEL CERTIFICADO.

Según lo definido en la DPC de Security Data.

4.4.1. Forma en la que se Acepta el Certificado.

El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el suscriptor y Security Data Seguridad en Datos y Firma Digital haya sido firmado.

Como evidencia de la aceptación deberá quedar un documento de aceptación firmado por el solicitante. El certificado se considerará válido a partir de la fecha en que se firmó el documento de aceptación.

4.4.2. Publicación del Certificado.

El certificado es publicado en los repositorios de Security Data, en un plazo máximo de 24 horas desde que se ha producido su emisión.

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

4.4.3. Notificación de la Emisión del Certificado por la AC a terceros.

No se efectúa notificación a terceros.

4.5. USO DE PARES DE CLAVES Y CERTIFICADOS.

4.5.1. Uso de la Clave Privada y del Certificado del Suscriptor.

Los certificados podrán ser utilizados según lo estipulado en esta PC y en la DPC.

4.5.2. Uso de Clave Pública y Certificado de la parte que confía.

Los terceros que confían en los certificados podrán utilizar los certificados para aquello que establece la presente PC y en la DPC.

Es responsabilidad de los terceros verificar el estado del certificado mediante los servicios ofrecidos por Security Data Seguridad en Datos y Firma Digital concretamente para ello y especificados en el presente documento.

4.6. RENOVACIÓN DE CERTIFICADOS.

Security Data no realiza la renovación de certificados, puesto que, el proceso de renovación se efectúa del mismo modo que la emisión de un nuevo certificado.

4.7. CAMBIO DE CLAVE DEL CERTIFICADO.

Según lo definido en la DPC de Security Data y la validación de identidad según lo definido en la presente PC.

4.7.1. Circunstancias para la Renovación del Certificado.

Se podrá renovar el certificado de Sello Electrónico bajo las siguientes circunstancias:

- El certificado ha caducado.
- El certificado ha sido revocado.

4.7.2. Personas autorizadas para solicitar renovación.

El formulario de solicitud de renovación debe ser firmado por el mismo suscriptor, ya fuera el propio suscriptor o el representante legal que tramita la solicitud del certificado.

Las circunstancias personales del suscriptor no deben haber variado, en especial su capacidad de representación legal.

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

4.7.3. Aprobación o rechazo de las solicitudes de renovación.

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.7.4. Notificación de la Renovación del Certificado.

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.7.5. Aceptación de la Renovación del Certificado.

Según lo definido en la DPC de Security Data.

4.7.6. Publicación del Certificado Renovado.

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.7.7. Notificación de la emisión de Certificados a otras entidades.

Security Data no realiza la notificación de emisión de certificados a otras entidades.

4.8. MODIFICACIÓN DE CERTIFICADOS.

No es aplicable.

4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.

Todo el proceso de revocación y suspensión se realizará conforme a la establecido en la DPC de Security Data.

4.10. SERVICIOS DE ESTADO DE CERTIFICADOS.

4.10.1. Características Operativas.

Security Data Seguridad en Datos y Firma Digital ofrece un servicio gratuito de publicación en Web de 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, la consulta se realiza mediante protocolo LDAP.

Las CRL se las puede descargar dentro de la página oficial <https://www.securitydata.net.ec/firma-electronica-en-ecuador/> en la opción de "Caducidad de Firma y CRL" URL: <https://www.securitydata.net.ec/firma-electronica-en-ecuador/>

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

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

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

4.10.2. Disponibilidad del Servicio.

Security Data ha puesto en práctica las siguientes medidas para garantizar la disponibilidad del servicio:

- Configuración redundante de sistemas informáticos, con el fin de evitar puntos únicos de fallos,
- Conexiones de alta velocidad redundantes con el fin de evitar la pérdida de servicio,
- Uso de sistemas de alimentación ininterrumpida.

A pesar de que esas medidas garantizan la disponibilidad del servicio de Security Data, no se puede garantizar una disponibilidad anual del 100%. Security Data tiene como objetivo proporcionar una disponibilidad del servicio anual del 99.6%.

4.10.3. Características Opcionales.

Sin estipulación.

4.11. FIN DE LA SUSCRIPCIÓN.

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

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES.

Security Data no almacena, ni tiene la posibilidad de almacenar la clave privada de los suscriptores y, por lo tanto, no presta servicio de recuperación de claves.

5. Controles de Instalaciones, Gestión y Operación.

Security Data implementará medidas técnicas y organizativas que garanticen:

- Seguridad física y lógica de las instalaciones.
- Control de accesos.
- Separación de funciones.
- Registro y monitoreo de eventos.
- Continuidad del servicio.

La aplicación de las prácticas se realizará de acuerdo a lo definido en la DPC de Security Data y procedimientos internos establecidos.

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

a) Control y Detección de Incidentes.

Cualquier interesado puede comunicar sus quejas o sugerencias a través de los siguientes medios:

- a. Por teléfono: 023922169.
- b. Por correo electrónico: info@securitydata.net.ec
- c. Cumplimentando el formulario electrónico disponible en el sitio web: <https://www.securitydata.net.ec/quejas-sugerencias-security-data/>

b) Registro de Incidentes.

Security Data dispone de un Registro de Incidentes en el que se inscribe toda incidencia que se haya producido con los certificados emitidos, y las evidencias obtenidas. Estos incidentes se registran, analizan y solucionan según los procedimientos del Sistema de Gestión de la seguridad de la Información de Security Data.

El Chief Technology Officer (CTO) determina la gravedad del incidente y nombra un responsable y, en caso de incidentes de seguridad relevantes, informa al Comité de Seguridad de la PKI.

5.1. CONTROLES DE SEGURIDAD FÍSICA.

Según lo definido en la DPC y DPS de Security Data.

5.2. CONTROLES DE PROCEDIMIENTO.

Según lo definido en la DPC y DPS de Security Data.

5.3. CONTROLES DE PERSONAL.

Según lo definido en la DPC y DPS de Security Data.

5.4. PROCEDIMIENTO 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 SECURITY DATA.
- Intentos de accesos no autorizados al sistema de archivos.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de SECURITY DATA.
- Encendido y apagado de la aplicación de SECURITY DATA.

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

- 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.

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.

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

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.

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 REGISTRO.

Según lo definido en la DPC y DPS de Security Data.

5.6. CAMBIO DE CLAVE.

Según lo definido en la DPC y DPS de Security Data.

5.7. COMPROMISO Y RECUPERACIÓN ANTE DESASTRES.

Según lo definido en la DPC y DPS de Security Data.

5.8. TERMINACIÓN DE CA.

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.

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	27

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.

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 y DPS de Security Data.

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

Los controles se estipulan según lo definido en la DPC y DPS de Security Data.

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

Los controles se estipulan según lo definido en la DPC y DPS de Security Data.

6.4. DATOS DE ACTIVACIÓN.

Los controles se estipulan según lo definido en la DPC y DPS de Security Data.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA.

Los controles se estipulan según lo definido en la DPC y DPS de Security Data.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA.

Los controles se estipulan según lo definido en la DPC y DPS de Security Data.

6.7. CONTROLES DE SEGURIDAD DE LA RED.

Los controles se estipulan según lo definido en la DPC y DPS de Security Data.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	28

6.8. SELLADO DE TIEMPO.

No aplica.

7. Perfiles de Certificados, CRL y OCSP.

7.1. PERFIL DEL CERTIFICADO.

Estos certificados sirven como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento. Security Data, en el marco de su servicio de certificados cualificados de sello electrónico, emite los siguientes tipos:

- **Certificado de Sello Electrónico para Persona Jurídica**, destinado a identificar a entidades privadas y garantizar la integridad y origen de los datos electrónicos.
- **Certificado de Sello Electrónico Institucional**, destinado a entidades u organismos públicos, cuando aplique.

Estos certificados pueden ser emitidos en los siguientes soportes:

- **En Archivo**, bajo custodia del titular, o
- **DSCF Dispositivo Seguro de Creación de Firma**, conforme a los requisitos de seguridad establecidos en la normativa vigente.

Con el objeto de identificar los certificados, Security Data ha asignado los siguientes identificadores de objeto (OID), según lo estipulado por la Normativa Técnica:

a) Sello electrónico en archivo:

Campo	en Archivo	Oblig.	Crit.	Observaciones
De SELLO ELECTRÓNICO	Autenticación y Firma			OID 1.3.6.1.4.1.oid_AC.2.4.1
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
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		SI		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	SI		OID 2.5.4.6
1.4.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	SI		OID 2.5.4.7
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

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

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		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 registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	SI		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) Titular de la Firma (Ciudad) ej. QUITO	SI		OID 2.5.4.7
1.6.3. Organization Name (O)	Nombre de la Persona Jurídica (Pública o Privada) Titular de la Firma. Ej. CORPORACION FAVORITA	SI		OID 2.5.4.10
1.6.4. Organization Unit Name (OU)	Se especifica el Departamento o Área al que pertenece el Signatario	No		OID 2.5.4.11
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) Titular de la Firma a la que está vinculado el Sello Electrónico"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
1.6.6. Serial Number	Número de Registro Único de Contribuyente de la Persona Jurídica (Pública o Privada) Ej. "1716151413001"	SI		OID 2.5.4.5
1.6.7. Common Name (CN)	Descripción del uso que se le dará al Sello Electrónico. Ej. RECEPCION DE DOCUMENTOS EN VENTANILLA UNICA	SI		OID 2.5.4.3
1.6.8. Surname	Apellidos del Signatario que estará vinculado al sello (como consta en el documento oficial)	SI		OID 2.5.4.4
1.6.9. Given Name	Nombres del Signatario que estará vinculado al sello (como consta en el documento oficial)	SI		OID 2.5.4.42
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
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública del Signatario	SI		Acorde ETSI TS 119 312
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)

CÓDIGO	SD-ID-PE-13
VERSIÓN	V2
FECHA DE APROBACIÓN	12/02/2026
PÁGINAS	30

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	Seleccionado "1"	SI		
2.3.3. Key Encipherment	Seleccionado "1"	SI		
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.102.2.4.1	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 SELLO ELECTRONICO EN ARCHIVO"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico) "info@example.com.ec"	SI		
2.6. Extended Key Usage		SI	NO	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	SI		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	NO		Sólo se activa si se incluye el correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico)
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		

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

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
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		

b) Sello electrónico en DSCF Dispositivo Seguro de Creación de Firma:

Campo	en Dispositivo Seguro de Creación de Firma DSCF	Oblig.	Crit.	Observaciones
De SELLO ELECTRÓNICO	Autenticación y Firma			OID 1.3.6.1.4.1.oid_AC.2.4.2
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
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		SI		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	SI		OID 2.5.4.6
1.4.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	SI		OID 2.5.4.7
1.4.3. Organization Name(O)	Nombre de la AC Subordinada "Organización"	SI		OID 2.5.4.10
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAIS)-IDENTIFICAR_ORGANIZACIÓN" Ej. VATEC-1716151413001	NO		2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
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		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 registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	SI		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) Titular de la Firma (Ciudad) ej. QUITO	SI		OID 2.5.4.7

1.6.3. Organization Name (O)	Nombre de la Persona Jurídica (Pública o Privada) Titular de la Firma. Ej. CORPORACION FAVORITA	SI		OID 2.5.4.10
1.6.4. Organization Unit Name (OU)	Se especifica el Departamento o Área al que pertenece el Signatario	No		OID 2.5.4.11
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) Titular de la Firma a la que está vinculado el Sello Electrónico"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
1.6.6. Serial Number	Número de Registro Único de Contribuyente de la Persona Jurídica (Pública o Privada) Ej. "1716151413001"	SI		OID 2.5.4.5
1.6.7. Common Name (CN)	Descripción del uso que se le dará al Sello Electrónico. Ej. RECEPCION DE DOCUMENTOS EN VENTANILLA UNICA	SI		OID 2.5.4.3
1.6.8. Surname	Apellidos del Signatario que estará vinculado al sello (como consta en el documento oficial)	SI		OID 2.5.4.4
1.6.9. Given Name	Nombres del Signatario que estará vinculado al sello (como consta en el documento oficial)	SI		OID 2.5.4.42
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
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública del Signatario	SI		Acorde ETSI TS 119 312
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	Seleccionado "1"	SI		
2.3.3. Key Encipherment	Seleccionado "1"	SI		
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"			

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

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.102.2.4.2	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 SELLO ELECTRONICO EN DISPOSITIVO SEGURO DE CREACION DE FIRMA - DSCF"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico) "info@example.com.ec"	SI		
2.6. Extended Key Usage		SI	NO	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	SI		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	NO		Sólo se activa si se incluye el correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico)
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	SI		OID 1.3.6.1.5.5.7.48.2
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]

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	34

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 sello electrónico 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 los certificados es:

- OID de archivo: 1.3.6.1.4.1.37746.2.4.1
- OID de DSCF: 1.3.6.1.4.1.37746.2.4.2

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.

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	35

7.1.8. Sintaxis y Semántica de los calificadores de Política.

Los certificados incluyen la extensión Certificate Policies con OID 2.5.29.32 con: un OID de política propio de SECURITY DATA para el tipo de certificado, y calificadores para documentar y explicar la política aplicable.

Calificadores soportados y significado:

- CPS URI con OID 1.3.6.1.5.5.7.2.1: URL pública al documento PC específica aplicable al certificado.
- User Notice con OID 1.3.6.1.5.5.7.2.2: texto informativo que describe el uso o el tipo del certificado.
- Sello Electrónico en Archivo
 - OID de política: 1.3.6.1.4.1.37746.102.2.4.1
 - CPS: <https://www.securitydata.net.ec/normativas/pcselloelectronico.pdf>
 - User Notice: "CERTIFICADO DE SELLO ELECTRONICO EN ARCHIVO"
- Sello Electrónico en DSCF
 - OID de política: 1.3.6.1.4.1.37746.102.2.4.2
 - CPS: <https://www.securitydata.net.ec/normativas/pcselloelectronico.pdf>
 - User Notice: "CERTIFICADO DE SELLO ELECTRONICO EN DISPOSITIVO SEGURO DE CREACION DE FIRMA - DSC"

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

En los certificados adjuntos, la extensión Certificate Policies con OID 2.5.29.32 se emite como NO crítica.

Si una aplicación/verificador no procesa Certificate Policies por ser no crítica, puede aceptar la cadena siguiendo validaciones estándar de firma, vigencia, revocación, ECU/KU, etc., siempre que el caso de uso no requiera validación por política.

Si el caso de uso requiere validación por política de sello electrónico, se debe comprobar que el certificado contiene el OID de política esperado para ese uso.

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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	36

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.

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.

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

- 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:
 - 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.

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

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 AC de la jerarquía 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 la AC 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 AC mantiene controles efectivos para asegurar razonablemente que:
 - La información del suscriptor es autenticada adecuadamente (para las actividades de registro realizadas por la AC), y
- c) **Controles generales.** Que la AC 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 AC 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 AC 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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	39

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.

9.1.1. Tarifas de Emisión o Renovación de certificados.

Los precios de los servicios de certificación o cualquier otro servicio serán facilitados a los clientes o posibles clientes por el Departamento Comercial de Security Data Seguridad en Datos y Firma Digital o por medio de la página web: www.securitydata.net.ec.

9.1.2. Tarifas de acceso al certificado.

El acceso a la clave pública de los certificados emitidos es gratuito, no obstante, la AC se reserva el derecho de imponer alguna tarifa para los casos de descarga masiva de certificados o cualquier otra circunstancia que a juicio de la AC deba ser gravada.

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

Security Data Seguridad en Datos y Firma Digital provee un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito, por medio de la publicación de las correspondientes CRL.

Security Data Seguridad en Datos y Firma Digital ofrece otros servicios de validación de certificados comerciales (como OCSP).

9.1.4. Tarifa por Otros Servicios.

Las tarifas aplicables a otros servicios se negociarán entre Security Data Seguridad en Datos y Firma Digital 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.

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

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 caso de defectos de funcionamiento por causas técnicas o por errores en los datos contenidos en el certificado, el suscriptor o el responsable del certificado puede mandar un correo a info@securitydata.net.ec a Security Data, informando del motivo de la devolución. Security Data verificará las causas de devolución, revocará el certificado emitido y procederá a emitir un nuevo certificado en un plazo máximo de 72 horas.

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

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.

La clave privada del titular es confidencial y de su exclusivo control; Security Data no tiene acceso a ella, pero protege la confidencialidad de los procesos de generación cuando ocurren en sus instalaciones.

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

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

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 (LOPD), su reglamento y demás disposiciones emitidas por la autoridad competente.

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

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.

Los titulares podrán ejercer sus derechos de acceso, eliminación, rectificación y oposición a través de los canales definidos en la Política de Privacidad publicada en el sitio web de Security Data.

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.

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

La revelación de datos personales a autoridades judiciales o administrativas se realizará previa verificación de la competencia de la autoridad solicitante y cumpliendo con el principio de proporcionalidad.

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

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

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, bajo su plena responsabilidad, 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 y a los estándares de aplicación. Además de:

- Emitir Certificados conforme a esta PC y a lo establecido en la DPC y a los estándares de aplicación.
- Emitir Certificados cuyo contenido mínimo sea definido en la PC y DPC vigentes.
- Emitir Certificados según la información que obra en su poder y libres de errores de entrada de datos.
- Mantener sus propias claves privadas bajo su exclusivo control empleando sistemas y productos fiables para almacenarlas de forma que garanticen su confidencialidad y los hagan inaccesibles a personas no autorizadas, evitando su pérdida o divulgación.
- Emitir los Certificados solicitados ajustándose según lo dispuesto en la DPC, en la PC y, en su caso, de los contratos de prestación de servicios de certificación correspondientes.
- Asimismo, emite los sellos electrónicos 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.
- Utilizar sistemas y productos fiables que estén protegidos contra alteración y que garanticen la seguridad técnica, y en su caso, criptografía de los procesos de certificación a los que sirven de soporte.
- Publicar los certificados emitidos según lo establecido en la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos.
- Proteger los datos personales según lo establecido en la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, y la Ley Orgánica de Protección de Datos Personales.
- Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos.

9.6.2. Declaraciones y Garantías de la RA.

Las responsabilidades de la entidad de registro son las siguientes:

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	44

- 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:

- Cumplir en todo momento con las normas y regulaciones emitidas por Security Data en su DPC y las correspondientes Políticas de Certificados.
- Comunicar a Security Data cualquier modificación o variación de los datos que se aportaron para obtener el Certificado de Sello Electrónico.
- Verificar, a través de la Lista de Certificados Revocados, el estado de los Certificados de sello electrónico.
- Proteger y conservar el Dispositivo Seguro de Creación de Firma. \o a su vez el acceso al certificado en software.
- La revocación del certificado y la emisión de uno nuevo a Security Data en caso de olvido de la clave de protección del Certificado de Sello Electrónico.
- Responder por el uso del Certificado de Sello Electrónico y de las consecuencias que se deriven de su utilización.
- Cumplir con lo estipulado en el artículo 17 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- 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.

Las responsabilidades de los terceros que confían son las siguientes:

- El tercero que confía es responsable de verificar el estado y la vigencia de los certificados digitales al momento de realizar cualquier transacción.
- El tercero que confía debe conocer y cumplir las obligaciones establecidas en la DPC y PC de la entidad de certificación.
- El tercero que confía se compromete a usar los certificados dentro de los términos establecidos en el marco de las leyes y normativas vigentes.
- El tercero que confía debe revisar las Listas de certificados revocados.

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	45

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.

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 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. 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.

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.

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	46

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 Protección de Datos Personales (LOPD) y su Reglamento; Código Orgánico de la Economía Social de los Conocimientos en lo relativo a propiedad intelectual. 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.

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.

	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	47

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.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO	CÓDIGO	SD-ID-PE-13
		VERSIÓN	V2
		FECHA DE APROBACIÓN	12/02/2026
		PÁGINAS	48

10. Control de Aprobaciones.

ELABORADO POR	COORDINADOR DEL SISTEMA DE GESTIÓN	
REVISADO POR	CHIEF TECHNOLOGY OFFICER (CTO)	
	SUPERVISOR LEGAL	
APROBADO POR	GERENTE GENERAL	