

CÓDIGO	SD-ID-PE-09
VERSIÓN	V13
FECHA DE APROBACIÓN	26/03/2026
PÁGINAS	1



DECLARACIÓN DE
PRÁCTICAS DE
CERTIFICACIÓN

marzo 26

2026



 www.securitydata.net.ec

 info@securitydata.net.ec

 392 2169 /  098 644 2122

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	2

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	FECHA	ELABORADO POR	REVISADO POR	APROBADO POR
V1	Edición Inicial	2/12/2025	Coordinador Legal	Gerente Técnico	Gerente General
V2	-	31/03/2011	Coordinador Legal	Gerente Técnico	Gerente General
V3	-	24/06/2011	Coordinador Legal	Gerente Técnico	Gerente General
V4	-	01/09/2011	Coordinador Legal	Gerente Técnico	Gerente General
V5	-	26/09/2011	Coordinador Legal	Gerente Técnico	Gerente General
V6	-	13/12/2011	Coordinador Legal	Gerente Técnico	Gerente General
V7	-	04/07/2011	Coordinador Legal	Gerente Técnico	Gerente General
V8	-	13/09/2013	Coordinador Legal	Gerente Técnico	Gerente General
V9	-	13/09/2019	Coordinador Legal	Gerente Técnico	Gerente General
V10	-	18/04/2022	Coordinador Legal	Gerente Técnico	Gerente General
V11	* Actualización del formato. * Actualización de los enlaces de certificados raíces.	29/11/2024	Coordinador de Calidad y Gestión	Gerente Técnico / Coordinador Legal	Gerente General
V12	* Actualización general de la DPC conforme a la Normativa Técnica. * Modificación del apartado Declaraciones y Garantías de la CA con respecto a la custodia de la información. * Actualización de enlaces para CRL y PC de certificados. * Actualización de las referencias a procedimientos conforme a los formalizados internamente.	25/02/2026	Coordinador del Sistema de Gestión	Chief Technology Officer (CTO) Supervisor Legal	Gerente General
V13	* Adaptación del documento al estándar RFC 3647. * Subsanación de las observaciones emitidas en el Oficio Nro. ARCOTEL-CTDS-2026-0296-OF por ARCOTEL.	26/03/2026	Coordinador del Sistema de Gestión	Chief Technology Officer (CTO) Supervisor Legal	Gerente General

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	3

Contenido

1.	INTRODUCCIÓN.....	12
1.1.	Descripción general.....	12
1.2.	Nombre e identificación del documento	13
1.2.1.	Identificación.....	13
1.3.	Participantes de la pki	13
1.3.1.	Entidad Acreditada (EA).	13
1.3.2.	Autoridad de Certificación (AC).....	13
1.3.3.	Autoridad de Certificación Raíz.	14
1.3.4.	Autoridades de Registro (AR).	14
1.3.5.	Tercero Vinculado.	14
1.3.6.	Solicitante.....	15
1.3.7.	Suscriptor.	15
1.3.8.	Firmante.	15
1.3.9.	Custodio de las claves.	15
1.3.10.	Tercero que confía en los certificados.	16
1.4.	Uso del certificado	16
1.4.1.	Usos apropiados de los certificados.....	16
1.4.2.	Usos prohibidos de los certificados.....	17
1.5.	ADMINISTRACIÓN DE LAS POLÍTICAS.....	19
1.5.1.	Organización que Administra el documento.....	19
1.5.2.	Persona de Contacto.	19
1.5.3.	Persona que determina la idoneidad de las DPC para la Política.....	20
1.5.4.	Procedimiento de aprobación de las DPC.	20
1.6.	DEFINICIONES Y ACRÓNIMOS.	20
2.	RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.	22
2.1.	Repositorios.....	22
2.2.	Publicación de información de certificación.	23
2.3.	Tiempo o frecuencia de publicación.	24
2.4.	Controles de acceso a los repositorios.....	25
3.	IDENTIFICACIÓN Y AUTENTICACIÓN.	25
3.1.	Denominación.	25
3.1.1.	Tipos de Nombres.	25
3.1.2.	Necesidad de que los nombres tengan significado.....	25

CÓDIGO	SD-ID-PE-09
VERSIÓN	V13
FECHA DE APROBACIÓN	26/03/2026
PÁGINAS	4

3.1.3.	Anonimato o seudónimo de los Suscriptores.	26
3.1.4.	Reglas para la interpretación de las distintas formas de nombres.	26
3.1.5.	Unicidad de los nombres.	26
3.1.6.	Reconocimiento, autenticación y función de las marcas.	26
3.1.7.	Resolución de conflictos relativos a nombres.	27
3.1.8.	Comprobación de las facultades de representación.	27
3.2.	Validación inicial de la identidad.	27
3.2.1.	Método para demostrar la posesión de la clave privada.	27
3.2.2.	Autenticación de la Identidad de la organización.	28
3.2.3.	Autenticación de la identidad individual.	28
3.2.4.	Información de suscriptor no verificada.	29
3.2.5.	Validación de la Autoridad.	29
3.2.6.	Criterios de Interoperabilidad.	30
3.3.	Identificación y autenticación en la renovación de claves.	30
3.3.1.	Identificación y autenticación para la renovación rutinaria de claves.	30
3.3.2.	Identificación y autenticación para la renovación de claves después de la revocación.	30
3.4.	Identificación y autenticación para la solicitud de revocación.	30
4.	REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO.	31
4.1.	Solicitud de certificados.	31
4.1.1.	Quién puede solicitar un Certificado.	31
4.1.2.	Proceso de inscripción y responsabilidades.	31
4.2.	Tramitación de solicitud de certificados.	32
4.2.1.	Realización de funciones de Identificación y Autenticación.	32
4.2.2.	Aprobación o rechazo de las solicitudes de certificados.	32
4.2.3.	Tiempo de tramitación de las solicitudes de certificados.	33
4.3.	Emisión del certificado.	33
4.3.1.	Acciones de la AC durante la Emisión de los Certificados.	33
4.3.2.	Notificación al suscriptor por parte de la CA de la Emisión del Certificado.	34
4.4.	Aceptación del certificado.	35
4.4.1.	Conducta que constituye la aceptación del certificado.	35
4.4.2.	Publicación del Certificado.	35
4.4.3.	Notificación de la emisión de certificados por parte de la CA a otras entidades.	35
4.5.	Usos de las claves y certificados.	35

CÓDIGO	SD-ID-PE-09
VERSIÓN	V13
FECHA DE APROBACIÓN	26/03/2026
PÁGINAS	5

4.5.1.	Uso de la Clave Privada y del Certificado del Suscriptor.....	35
4.5.2.	Uso de la Clave Pública y Certificado de la parte que confía.....	36
4.5.3.	Especificaciones técnicas de los algoritmos y tamaños de clave.....	36
4.5.4.	Generación de claves.....	36
4.6.	Renovación del certificado.....	37
4.6.1.	Circunstancias para la renovación del certificado.....	37
4.6.2.	Quién puede solicitar la renovación.....	37
4.6.3.	Tramitación de solicitudes de renovación de certificados.....	37
4.6.4.	Notificación de la emisión de un nuevo certificado al suscriptor.....	37
4.6.5.	Conducta que constituye aceptación de un certificado de renovación.....	37
4.6.6.	Publicación del certificado de renovación por parte de la CA.....	37
4.6.7.	Notificación de la emisión de certificados por parte de la CA a otras entidades.....	37
4.7.	Cambio de clave del certificado.....	37
4.7.1.	Circunstancias para la renovación de la clave del certificado.....	37
4.7.2.	Quién puede solicitar la certificación de una nueva clave pública.....	38
4.7.3.	Procesamiento de solicitudes de Renovación de Claves de certificados.....	38
4.7.4.	Notificación de la emisión de un nuevo certificado al Suscriptor.....	38
4.7.5.	Conducta que constituye aceptación de un certificado con nueva clave.....	38
4.7.6.	Publicación del certificado con nueva clave por parte de la CA.....	39
4.7.7.	Notificación de la emisión del certificado por la AC a otras entidades.....	39
4.8.	Modificación de certificados.....	39
4.8.1.	Circunstancias para la Modificación del Certificado.....	39
4.8.2.	Quién puede solicitar la modificación del certificado.....	39
4.8.3.	Procesamiento de solicitudes de modificación de certificados.....	39
4.8.4.	Notificación de la emisión de un nuevo certificado al suscriptor.....	40
4.8.5.	Conducta que constituye aceptación del certificado modificado.....	40
4.8.6.	Publicación del certificado modificado por la CA.....	40
4.8.7.	Notificación de la emisión del certificado por la CA a otras entidades.....	40
4.9.	Revocación y suspensión del certificado.....	40
4.9.1.	Circunstancia de Revocación.....	40
4.9.2.	Quién puede Solicitar la Revocación.....	42
4.9.3.	Procedimientos para la Solicitud de Revocación.....	42
4.9.4.	Plazo de gracia para la solicitud de Revocación.....	45
4.9.5.	Plazo en el que la CA debe tramitar la solicitud de Revocación.....	45

CÓDIGO	SD-ID-PE-09
VERSIÓN	V13
FECHA DE APROBACIÓN	26/03/2026
PÁGINAS	6

4.9.6.	Requisito de comprobación de Revocación para las Partes que Confían.	45
4.9.7.	Frecuencia de Emisión de CRLs.	45
4.9.8.	Latencia máxima para CRL.	46
4.9.9.	Disponibilidad de comprobación de estado/revocación en línea.....	46
4.9.10.	Requisitos de Comprobación de Revocación en Línea.....	46
4.9.11.	Otras formas de anuncios de revocación disponibles.....	46
4.9.12.	Requisitos especiales en materia de Compromiso de Claves.	46
4.9.13.	Circunstancias de Suspensión.	46
4.9.14.	Quién puede Solicitar la Suspensión.	47
4.9.15.	Procedimiento para solicitud de suspensión.	47
4.9.16.	Límites del Periodo de Suspensión.....	47
4.10.	Servicios de estado de certificados.	47
4.10.1.	Características Operativas.....	47
4.10.2.	Disponibilidad del Servicio.	48
4.10.3.	Características Opcionales.	48
4.11.	Fin de la suscripción.	48
4.12.	Custodia y recuperación de claves.	49
4.12.1.	Política y prácticas de depósito y recuperación de claves.	49
4.12.2.	Política y prácticas de encapsulación y recuperación de claves de sesión.	49
5.	CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIÓN.....	49
5.1.	Controles físicos.	49
5.1.1.	Ubicación del sitio y construcción.....	49
5.1.2.	Acceso Físico.....	50
5.1.3.	Energía y Aire Acondicionado.	50
5.1.4.	Exposiciones al Agua.	50
5.1.5.	Protección y Prevención de Incendios.	50
5.1.6.	Almacenamiento de medios.	50
5.1.7.	Eliminación de residuos.....	51
5.1.8.	Copia de Seguridad externa.	51
5.2.	Controles de procedimiento.	51
5.2.1.	Roles de Confianza.	51
5.2.2.	Número de personas necesarias por tarea.	52
5.2.3.	Identificación y autenticación por cada rol.....	52
5.2.4.	Funciones que requieren separación de funciones.	52

CÓDIGO	SD-ID-PE-09
VERSIÓN	V13
FECHA DE APROBACIÓN	26/03/2026
PÁGINAS	7

5.3.	Controles de personal.....	52
5.3.1.	Requisitos sobre la Cualificación, Experiencia y Conocimientos Profesionales..	52
5.3.2.	Procedimiento de verificación de Antecedentes.....	53
5.3.3.	Requisitos de Formación.....	53
5.3.4.	Frecuencia y requisitos de reentrenamiento.....	53
5.3.5.	Frecuencia y Secuencia de Rotación de Tareas.....	53
5.3.6.	Sanciones por acciones No Autorizadas.....	53
5.3.7.	Requisitos de contratista independiente.....	54
5.3.8.	Documentación suinistrada al Personal.....	54
5.4.	Procedimientos de registro de auditoría.....	54
5.4.1.	Tipos de Eventos Registrados.....	54
5.4.2.	Frecuencia del procesamiento de Registro.....	55
5.4.3.	Periodo de Conservación de los Registros de Auditoría.....	55
5.4.4.	Protección del registro de auditoría.....	55
5.4.5.	Procedimientos de copia de seguridad del Registro de Auditoría.....	56
5.4.6.	Sistema de recopilación de Auditorías.....	56
5.4.7.	Notificación al sujeto causante del evento.....	56
5.4.8.	Evaluaciones de Vulnerabilidades.....	56
5.5.	Archivo de registro.....	56
5.5.1.	Tipo de registros Archivados.....	56
5.5.2.	Periodo de Conservación de los datos archivados.....	57
5.5.3.	Protección del Archivo.....	57
5.5.4.	Procedimientos de Copia de Seguridad del Archivo.....	57
5.5.5.	Requisitos para el Sellado de Tiempo de los Registros.....	57
5.5.6.	Sistema de recopilación de archivos.....	57
5.5.7.	Procedimientos para obtener y verificar información de archivo.....	57
5.6.	Cambio de clave.....	58
5.7.	Compromiso y recuperación ante desastres.....	58
5.7.1.	Procedimientos de manejo de incidentes y compromisos.....	58
5.7.2.	Los recursos informáticos, el software y/o los datos están dañados.....	58
5.7.3.	Procedimientos de compromiso de la Clave Privada de la entidad.....	58
5.7.4.	Capacidades de continuidad del negocio después de un desastre.....	59
5.8.	Terminación de CA o RA.....	59
6.	CONTROLES TÉCNICOS DE SEGURIDAD.....	60

CÓDIGO	SD-ID-PE-09
VERSIÓN	V13
FECHA DE APROBACIÓN	26/03/2026
PÁGINAS	8

6.1.	Generación e instalación de pares de claves.	60
6.1.1.	Generación de pares de claves.....	60
6.1.2.	Entrega de la Clave Privada al Suscriptor.	60
6.1.3.	Entrega de la Clave Pública al Emisor del Certificado.	61
6.1.4.	Entrega de la Clave Pública de la AC a partes confiables.	61
6.1.5.	Tamaños de clave.	61
6.1.6.	Generación de parámetros de clave pública y control de calidad.	61
6.1.7.	Usos Admitidos de la Clave (campo KeyUsage de X.509v3).	62
6.2.	Protección de claves privadas e ingeniería de módulos criptográficos.	62
6.2.1.	Estándares para los Módulos Criptográficos.....	62
6.2.2.	Control Multipersona (k de n) de la Clave Privada.....	62
6.2.3.	Custodia de la Clave Privada.	62
6.2.4.	Copia de Seguridad de la Clave Privada de la AC.	62
6.2.5.	Archivado de Claves Privadas.....	63
6.2.6.	Transferencia de la Clave Privada hacia o desde el Módulo Criptográfico.	63
6.2.7.	Almacenamiento de clave privada en el módulo criptográfico.	63
6.2.8.	Método de Activación de la Clave Privada.....	64
6.2.9.	Método de Desactivación de la Clave Privada.	64
6.2.10.	Método de Destrucción de la Clave Privada.	64
6.2.11.	Clasificación del módulo criptográfico.	64
6.3.	Otros aspectos de la gestión de pares de claves.....	65
6.3.1.	Archivo de la Clave Pública.....	65
6.3.2.	Periodos operativos de los Certificados y Periodo de uso del Par de Claves.....	65
6.4.	Datos de activación.	65
6.4.1.	Generación e Instalación de los Datos de Activación.	65
6.4.2.	Protección de los Datos de Activación.	65
6.4.3.	Otros aspectos de los datos de activación.	65
6.5.	Controles de seguridad informática.....	65
6.5.1.	Requisitos técnicos de seguridad informática.	66
6.5.2.	Clasificación de la Seguridad Informática.	66
6.6.	Controles técnicos del ciclo de vida.	66
6.6.1.	Controles de Desarrollo de Sistemas.	66
6.6.2.	Controles de Gestión de Seguridad.....	67
6.6.3.	Controles de Seguridad del Ciclo de Vida.	68

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	9

6.7.	Controles de seguridad de la red.	68
6.8.	Sellado de tiempo.	68
7.	PERFILES DE LOS CERTIFICADOS CRL Y OCSP.	69
7.1.	Perfil de los certificados.	69
7.1.1.	Número de Versión.	75
7.1.2.	Extensión de los Certificados (OID-Objeto Identificador).	76
7.1.3.	Identificadores de objetos de algoritmo.	76
	Para la emisión y validación del certificado, la AC emplea los siguientes Identificadores de Objeto (OID) asociados a los algoritmos criptográficos utilizados:.....	76
7.1.4.	Formas de los nombres.	77
7.1.5.	Restricciones de nombre.....	77
7.1.6.	Identificador de objeto de Política de Certificado.	77
7.1.7.	Uso de la extensión Restricciones de política.	77
	No se estipula.....	77
7.1.8.	Sintaxis y semántica de los calificadores de políticas.	77
7.1.9.	Semántica de procesamiento para la extensión de políticas de certificados críticos. 78	
	No se estipula.....	78
7.2.	Perfil CRL.	78
7.2.1.	Número de Versión.	78
7.2.2.	CRL y Extensiones de entrada CRL.	78
	CRL de la Autoridad Raíz (AC Root).	78
	CRL de las Autoridades de Certificación Subordinadas.....	79
7.3.	Perfil OCSP.....	79
7.3.1.	Número(s) de versión.....	79
7.3.2.	Extensiones OCSP.....	79
8.	AUDITORÍAS DE CUMPLIMIENTO Y OTRAS EVALUACIONES.	81
8.1.	Frecuencia o circunstancias de la evaluación.	81
8.2.	Cualificación del auditor.....	81
8.3.	Relación entre el auditor y la entidad auditada.....	81
8.4.	Temas cubiertos por la evaluación.....	82
8.5.	Acciones adoptadas como resultado de la deficiencia.	83
8.6.	Comunicación de resultados.	83
9.	OTROS ASUNTOS LEGALES Y DE ACTIVIDAD.	83
9.1.	Tarifas.....	83

CÓDIGO	SD-ID-PE-09
VERSIÓN	V13
FECHA DE APROBACIÓN	26/03/2026
PÁGINAS	10

9.1.1.	Tarifas de Emisión o renovación de Certificados.	83
9.1.2.	Tarifas de Acceso a los Certificados.	84
9.1.3.	Tarifas de Acceso a la Información de Estado o Revocación.	84
9.1.4.	Tarifas por Otros Servicios.	84
9.1.5.	Política de reembolso.....	84
9.2.	Responsabilidad financiera.	85
9.2.1.	Cobertura del Seguro.	85
9.2.2.	Otros activos.....	85
9.2.3.	Cobertura de seguro o garantía para entidades finales.....	85
9.3.	Confidencialidad de la información empresarial.	85
9.3.1.	Alcance de la Información Confidencial.....	86
9.3.2.	Información no Confidencial.	86
9.3.3.	Responsabilidad en la Protección de Información Confidencial.....	86
9.4.	Privacidad de la información personal.....	87
9.4.1.	Política de Privacidad.	87
9.4.2.	Información tratada como Privada.	87
9.4.3.	Información no considerada Privada.	87
9.4.4.	Responsabilidad de proteger la información privada.	87
9.4.5.	Aviso y Consentimiento para el uso de información privada.....	87
9.4.6.	Divulgación en virtud de un proceso judicial o administrativo.....	88
9.4.7.	Otras circunstancias de revelación de información.	88
9.5.	Derechos de propiedad intelectual.....	88
9.6.	Declaraciones y garantías.....	88
9.6.1.	Declaraciones y Garantías de la CA.	88
9.6.2.	Declaraciones y Garantías de la RA.	90
9.6.3.	Declaraciones y Garantías de los Solicitantes.	91
9.6.4.	Declaraciones y Garantías de los Suscriptores.....	91
9.6.5.	Declaraciones y Garantías de la parte que Confía.	92
9.6.6.	Declaraciones y Garantías de los Usuarios.....	92
9.7.	Renuncias a garantías.....	95
9.8.	Limitaciones de responsabilidad.....	95
9.9.	Indemnizaciones.....	95
9.10.	Plazo y terminación.....	95
9.10.1.	Plazo.	95

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	11

9.10.2.	Terminación.....	95
9.11.	Avisos y comunicaciones individuales con los participantes.	96
9.12.	Enmiendas.	96
9.13.	Disposiciones de resolución de disputas.....	96
9.14.	Ley aplicable.	96
9.15.	Cumplimiento de la legislación aplicable.	97
9.16.	Disposiciones diversas.....	97
9.16.1.	Acuerdo Completo.	97
9.16.2.	Cesión.....	97
9.16.3.	Divisibilidad.	97
9.16.4.	Ejecución.	97
9.16.5.	Fuerza Mayor.	97
9.17.	Otras disposiciones.	97
10.	CONTROL DE APROBACIONES.	97

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	12

1. INTRODUCCIÓN.

1.1. Descripción general

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

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

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

En esta Declaración de Prácticas de Certificación se especifican las condiciones, políticas y procedimientos aplicables a la solicitud, emisión, uso, suspensión y revocación de los certificados de firma electrónica, así como para la prestación de servicios relacionados y contiene:

1. Datos de identificación de la Entidad de Certificación de Información y Servicios Relacionados de la acreditada.
2. Condiciones de manejo de la información suministrada por los usuarios.
3. Límites de responsabilidad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.
4. Obligaciones de la Entidad de Certificación de Información y Servicios Relacionados Acreditada en la prestación de servicios de certificación de información y servicios relacionados con la firma.
5. Obligaciones de los usuarios y precauciones que deben observarse en el manejo, uso y custodia de certificados y claves.
6. Políticas de manejo de los certificados de firma electrónica.
7. Políticas y condiciones de manejo de servicios relacionados con firma electrónica.
8. Garantías en el cumplimiento de las obligaciones que se deriven de sus actividades.
9. Costos y Tarifas de los servicios de certificación de información y servicios relacionados con la firma electrónica.

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

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	13

1.2. Nombre e identificación del documento

1.2.1. Identificación.

Nombre:	Declaración de Practicas de Certificación (DPC)
Versión:	12
Descripción:	Declaración de Practicas de Certificación de Security Data Seguridad en Datos y Firma Digital S.A.
Fecha de Emisión:	25 de febrero del 2026
Sitio Web:	www.securitydata.net.ec
Nombre Sociedad:	Security Data Seguridad en Datos y Firma Digital S.A.
Código Postal:	170528
Correo electrónico:	info@securitydata.net.ec
Dirección:	Alonso de Torres y Av. Del Parque oficinas administrativas C8
Número de teléfono:	023922169
Sitio Web:	www.securitydata.net.ec
OID:	1.3.6.1.4.1.37746.1

1.2.2. Publicación.

Este documento puede obtenerse libremente en la dirección electrónica:

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

1.3. Participantes de la PKI

1.3.1. Entidad Acreditada (EA).

Security Data Seguridad en Datos y Firma Digital es un Entidad Acreditada (EA) que emite certificados reconocidos según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Security Data Seguridad en Datos y Firma Digital es la entidad emisora de los certificados y responsable de las operaciones del ciclo de vida de los certificados. Las funciones de autorización, registro, emisión y revocación respecto de los certificados personales de entidad final, pueden ser realizadas por otras entidades por delegación soportada contractualmente con Security Data Seguridad en Datos y Firma Digital, que actuarán como intermediarios. Security Data Seguridad en Datos y Firma Digital también ofrece servicios de validación de firmas electrónicas, sello electrónico y de sellado de tiempo, regidos por sus políticas particulares, no incluidas en este documento, podrá emitir a solicitud del interesado o de oficio, un documento informativo del estado del certificado. Este documento certificará la vigencia, revocación o suspensión de la firma electrónica a una fecha y hora determinada, otorgando certeza jurídica sobre el estado del ciclo de vida del certificado ante terceros.

1.3.2. Autoridad de Certificación (AC).

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

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	14

1.3.3. Autoridad de Certificación Raíz.

Se denomina Autoridad de Certificación Raíz (CA Root) a la entidad dentro de la jerarquía que emite certificados a otras autoridades de certificación, y cuyo certificado de clave pública ha sido autofirmado. Su función es firmar el certificado de las otras ACs pertenecientes a la Jerarquía de Certificación.

1.3.4. Autoridades de Registro (AR).

Security Data Seguridad en Datos y Firma Digital como autoridad de registro, es la responsable de realizar la verificación de identidad de los solicitantes de certificados digitales, así como de validar, aprobar o rechazar las solicitudes de emisión, renovación, revocación o suspensión de dichos certificados, para ello, empleará sistemas de biometría avanzada y detección de prueba de vida (liveness check). En aquellos casos donde el sistema biométrico no alcance el umbral de confianza requerido, o existan inconsistencias en los datos, la AR aplicará obligatoriamente un protocolo de Validación Reforzada, el cual consiste en:

- Presencialidad: El solicitante deberá comparecer físicamente en las oficinas o centros de atención autorizados.
- Video de validación: En su defecto, se solicitará un video de validación de identidad mencionando la información requerida.

1.3.5. Tercero Vinculado.

Un Tercero Vinculado de Security Data Seguridad en Datos y Firma Digital, es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado.
- Gestionar la generación de claves y la emisión del certificado.
- Hacer entrega de las instrucciones para la emisión del certificado al suscriptor y, de ser el caso, hacer entrega del dispositivo criptográfico.

Podrán actuar como Tercero Vinculado de Security Data Seguridad en Datos y Firma Digital:

- Cualquier entidad de confianza que llegue a un acuerdo con Security Data Seguridad en Datos y Firma Digital para actuar como tercero en nombre de Security Data Seguridad en Datos y Firma Digital. Estos actuarán como extensión de la Autoridad de Registro y están sujetos a las mismas auditorías y niveles de seguridad que la oficina matriz.
- La propia Security Data Seguridad en Datos y Firma Digital directamente.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	15

Security Data Seguridad en Datos y Firma Digital formalizará contractualmente las relaciones entre ella y cada una de las entidades que actúen como Tercero Vinculado de Security Data; posteriormente la vinculación se formalizará mediante el respectivo registro del ente de control.

La entidad que actúe como Tercero Vinculado de Security Data podrá autorizar a una o varias personas como Operador del Tercero Vinculado para operar con el sistema informático de emisión de certificados de Security Data en nombre del Tercero Vinculado.

Allí donde la ubicación geográfica de los suscriptores represente un problema logístico para la identificación del suscriptor y en la solicitud y entrega de certificados, el Tercero Vinculado o Security Data podrá delegar estas funciones a otra entidad o persona de confianza denominada agente móvil o distribuidor autorizado. Dicha entidad o persona deberá tener una especial vinculación con el Tercero Vinculado o con Security Data y una relación de proximidad con los suscriptores de los certificados que justifique la delegación. La entidad o persona de confianza deberá firmar un acuerdo de colaboración con el Tercero Vinculado o con Security Data en el que se acepte la delegación de estas funciones. Security Data Seguridad en Datos y Firma Digital deberá conocer y autorizar de manera expresa el acuerdo.

1.3.6. Solicitante.

Solicitante es la persona natural que, en nombre propio o en presentación de un tercero, solicita la emisión de un certificado a Security Data Seguridad en Datos y Firma Digital. Los requisitos que debe reunir un solicitante dependerán del tipo de certificado solicitado y estarán recogidos en la "Política de Certificación" de cada tipo de certificado concreto.

1.3.7. Suscriptor.

El Suscriptor es la persona natural o jurídica que ha contratado los servicios de certificación de Security Data Seguridad en Datos y Firma Digital. Por lo tanto, será el propietario del certificado.

1.3.8. Firmante.

El Firmante es la persona que posee un dispositivo de creación de firma o el acceso al certificado de firma en software y que actúa en nombre propio o en nombre de una persona jurídica a la que representa.

El Firmante será responsable de custodiar los datos de creación de firma, es decir, la clave privada asociada al certificado.

1.3.9. Custodio de las claves.

La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica, será responsabilidad de la persona natural solicitante, cuya identificación se incluirá en el certificado electrónico.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	16

1.3.10. Tercero que confía en los certificados.

Se entiende como tercero que confía en los certificados (en inglés, relaying party) a toda persona u organización que voluntariamente confía en un certificado emitido por Security Data Seguridad en Datos y Firma Digital.

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

Las obligaciones y responsabilidades de Security Data con terceros que, voluntariamente confíen en los certificados, se limitarán a las recogidas en esta DPC.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

1.4. Uso del certificado

1.4.1. Usos apropiados de los certificados.

El certificado de firma electrónica debe usarse para identificar al firmante, dar validez jurídica a documentos electrónicos, garantizar autenticidad e integridad, y permitir la verificación y responsabilidad sobre lo firmado.

Certificados de persona natural.

Los usos apropiados para los certificados de persona natural son los siguientes:

- La suscripción de documentos electrónicos en nombre propio, en el marco de actos jurídicos lícitos;
- La aceptación de contratos, declaraciones, formularios y cualquier otro documento electrónico que requiera manifestación de voluntad;
- La realización de trámites electrónicos ante entidades públicas o privadas;
- La validación de identidad en plataformas digitales autorizadas;
- La suscripción de documentos en calidad de representante legal, siempre que cuente con facultades suficientes y debidamente acreditadas;
- Cualquier otro uso permitido por la normativa ecuatoriana aplicable en materia de comercio electrónico y firma electrónica y esta DPC.

Certificados de persona jurídica para representante legal.

La firma electrónica emitida a favor de una persona natural en calidad de representante legal deberá ser utilizada exclusivamente dentro del ámbito de sus facultades legales y para fines lícitos, incluyendo:

- La suscripción de documentos electrónicos en nombre y representación de la organización a la cual representa;

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	17

- La celebración, aceptación y ejecución de actos jurídicos, contratos, acuerdos y declaraciones vinculantes para la organización representada;
- La realización de trámites electrónicos ante entidades públicas o privadas en ejercicio de su representación legal;
- La validación de identidad en plataformas tecnológicas, en calidad de representante legal debidamente acreditado;
- La firma de documentos relacionados con obligaciones legales, regulatorias, administrativas, comerciales o laborales de la entidad representada;
- Cualquier otro uso permitido por la normativa ecuatoriana aplicable, dentro del marco de sus atribuciones legales o estatutarias o de esta DPC.

Certificados de persona jurídica para miembro de empresa.

La firma electrónica asignada a un miembro de empresa deberá ser utilizada exclusivamente en el marco de sus funciones laborales o contractuales y conforme a las políticas internas de la organización, incluyendo:

- La suscripción de documentos electrónicos relacionados con sus funciones, responsabilidades o actividades asignadas.
- La ejecución de procesos digitales dentro de los sistemas corporativos que requieran autenticación mediante firma electrónica.
- La gestión de trámites administrativos, operativos o comerciales en nombre de la empresa, cuando esté debidamente autorizado.
- La interacción con plataformas tecnológicas de terceros en representación de la empresa, dentro del alcance de sus funciones.
- Cualquier otro uso expresamente autorizado por la empresa y permitido por la normativa vigente.

1.4.2. Usos prohibidos de los certificados.

Certificados de persona natural.

Los usos prohibidos para los certificados de persona natural son los siguientes:

- Utilizar la firma electrónica para suplantar la identidad de terceros o actuar sin autorización.
- Compartir, ceder, transferir o permitir el uso de su firma electrónica, credenciales, claves privadas o mecanismos de autenticación a terceros.
- Utilizar la firma electrónica para fines ilícitos, fraudulentos o contrarios a la ley, la moral o el orden público.
- Firmar documentos en nombre de terceros sin contar con la debida autorización legal o mandato vigente.
- Alterar, manipular o intentar vulnerar los mecanismos de seguridad asociados a la firma electrónica.
- Utilizar la firma electrónica en sistemas no autorizados o que no garanticen condiciones adecuadas de seguridad.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	18

- Desconocer o repudiar documentos válidamente firmados, salvo prueba de uso indebido o compromiso de seguridad.

Certificados de persona jurídica para representante legal.

El titular de la firma electrónica de representante legal se obliga a abstenerse de:

- Utilizar la firma electrónica fuera del ámbito de sus facultades legales o excediendo los límites de su representación.
- Firmar documentos en nombre de la persona jurídica sin contar con facultades vigentes o debidamente inscritas.
- Compartir, ceder, transferir o permitir el uso de su firma electrónica, certificados digitales, claves privadas o credenciales a terceros.
- Utilizar la firma electrónica para fines personales cuando esta haya sido emitida para actuar en representación de una persona jurídica, salvo que exista habilitación expresa.
- Utilizar la firma electrónica para fines ilícitos, fraudulentos o contrarios a la normativa vigente.
- Suplantar la identidad de otros representantes o actuar sin autorización válida.
- Alterar, manipular o vulnerar los mecanismos de seguridad asociados a la firma electrónica.
- Continuar utilizando la firma electrónica en caso de pérdida de la calidad de representante legal, revocatoria de poderes o extinción de la persona jurídica.
- Desconocer o repudiar documentos electrónicos válidamente firmados dentro del ámbito de sus facultades, salvo prueba de uso indebido o compromiso de seguridad.

Certificados de persona jurídica para miembro de empresa.

El titular de la firma electrónica se obliga a abstenerse de:

- Utilizar la firma electrónica para fines personales o ajenos a sus funciones dentro de la empresa.
- Firmar documentos sin contar con autorización, competencia o delegación correspondiente.
- Exceder los límites de sus funciones o atribuciones al utilizar la firma electrónica.
- Compartir, ceder o permitir el uso de su firma electrónica, credenciales o claves a terceros, incluso dentro de la empresa.
- Utilizar la firma electrónica para fines ilícitos, fraudulentos o contrarios a las políticas internas o normativa aplicable.
- Alterar, manipular o vulnerar los mecanismos de seguridad asociados a la firma electrónica.
- Utilizar la firma electrónica fuera de los sistemas o plataformas autorizadas por la empresa.
- Continuar utilizando la firma electrónica en caso de suspensión, cambio de funciones, terminación de la relación laboral o revocatoria de autorización.
- Desconocer o repudiar documentos electrónicos válidamente firmados dentro del ámbito de sus funciones, salvo prueba de uso indebido.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	19

1.5. ADMINISTRACIÓN DE LAS POLÍTICAS.

La Declaración de Prácticas de Certificación – DPC de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. - y otra documentación relevante son publicadas en: <https://www.securitydata.net.ec/ayuda-security-data-ecuador/>.

Todas las modificaciones relevantes en la documentación de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A., serán comunicadas al Arcotel y las nuevas versiones del documento serán publicadas en el mismo sitio web.

1.5.1. Organización que Administra el documento.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. con RUC 1792261848001, es la entidad que administra y es autora de la presente DPC, Políticas de Certificación y demás documentos normativos.

El responsable del documento y su aprobación es:

- **Nombres:** Cesar Santana Villamar
- **Cargo:** Gerente general
- **Correo electrónico:** info@securitydata.net.ec

1.5.2. Persona de Contacto.

La Entidad de Certificación establecerá mecanismos formales para la atención de consultas específicas relacionadas con el contenido, alcance, interpretación y aplicación de la presente Declaración de Prácticas de Certificación (DPC).

La recepción de consultas se efectuará en días laborables, de lunes a viernes, en horario de 09h00 a 17h00. Para su tramitación, el solicitante deberá realizar una notificación previa por correo electrónico y, adicionalmente, remitir un oficio físico dirigido a la oficina matriz de la Entidad de Certificación.

Persona contacto: Lenin Alberto Vásquez Gonzalez
Correo electrónico: cto@securitydata.net.ec
Dirección: Alonso de Torres y Av. Del Parque Oficinas Administrativas C8.
Número de teléfono: 023922169
Sitio Web: www.securitydata.net.ec

La fecha de recepción del oficio físico en la oficina matriz constituirá el inicio formal del cómputo del plazo de respuesta.

La Entidad de Certificación dará respuesta a las consultas por medios electrónicos, dentro de un plazo máximo de quince (15) días contados a partir de la recepción del oficio físico.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	20

Cuando la naturaleza de la consulta así lo requiera, la Entidad de Certificación podrá solicitar información o documentación complementaria para su adecuada atención, conforme a sus procedimientos internos y a la normativa aplicable.

Frecuencia de Revisión.

La DPC y las distintas PCs serán revisadas y si procede, actualizadas anualmente o cuando se presente algún cambio.

1.5.3. Persona que determina la idoneidad de las DPC para la Política.

El presente documento es firmado digitalmente por el Responsable de la AC de Security Data antes de ser publicado, y es el encargado de evaluar y aprobar que su contenido sea adecuado, suficiente y coherente con los servicios prestados, los requisitos establecidos en la RFC 3647, así como con la normativa legal y regulatoria aplicable.

1.5.4. Procedimiento de aprobación de las DPC.

La publicación de las revisiones de esta DPC y de las Políticas de Certificados de cada tipo de certificados deberá ser aprobada por la Dirección General de Security Data Seguridad en Datos y Firma Digital, después de comprobar el cumplimiento de los requisitos expresados en ella.

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.

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.

Certificado Reconocido: Certificado expedido por una Entidad Acreditada que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes, y a la fiabilidad y las garantías de los servicios de certificación que presten.

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.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	21

Datos de Creación de Firma (Clave Privada): Son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la firma electrónica.

Datos de Verificación de Firma (Clave Pública): Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

Dispositivo Seguro de Creación de Firma (DSCF): Instrumento que sirve para aplicar los datos de creación de firma.

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

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

Sello electrónico: Es un mensaje de datos que identifica a la persona jurídica pública o privada que es titular de la firma y su vinculación con el signatario, quien es responsable de su protección y custodia.

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

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

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

Validación Reforzada: Procedimiento excepcional de verificación de identidad mediante presencia física o video de validación donde mencione información que permita validar la identidad del suscriptor, cuando los medios automáticos no son concluyentes.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	22

Detección de Prueba de Vida: Tecnología destinada a determinar si la muestra biométrica proviene de una persona viva y presente en el momento de la captura, y no de una reproducción.

Acrónimos.

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

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.

2.1. Repositorios.

Los repositorios de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A están referenciados en la <https://consultacertificados.securitydata.net.ec/app-consulta-certificados/#/consultarCert>. Cualquier cambio en las URLs se notificará a todas entidades que puedan verse afectadas. Las direcciones IP correspondientes a cada URL podrán ser múltiples y dinámicas, pudiendo ser modificadas sin previo aviso.

Declaración de Prácticas de Certificación:

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

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	23

PC Persona Natural: https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/Politicasy20de%20Certificado%20Persona%20Natural.pdf

PC Representante Legal: https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/Politicasy20de%20Certificado%20Representante%20Legal.pdf

PC Miembro de Empresa: https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/Politicasy20de%20Certificado%20Miembro%20de%20Empresa.pdf

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

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

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

2.2. Publicación de información de certificación.

Políticas y Prácticas de Certificación.

Tanto la DPC actual, como las Políticas de Certificación de cada tipo de certificado, estarán disponibles en formato electrónico en la Web de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.

Las versiones anteriores serán retiradas de su consulta on-line, pero podrán ser solicitadas por los interesados en la dirección de contacto de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.

Términos y Condiciones.

La relación contractual entre SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A y los Suscriptores, está basada en la firma de un Contrato de Prestación de Servicios de Certificación y la aceptación de las Condiciones Generales de Contratación de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A publicadas en su web.

Difusión de los Certificados.

El Suscriptor del certificado será el responsable de hacer llegar su certificado a todo aquel tercero que desee autenticar a un usuario o comprobar la validez de una firma. Este envío se

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	24

realizará generalmente de manera automática, adjuntando el certificado a todo documento firmado electrónicamente.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A publica en su página web, de forma permanente e ininterrumpida los certificados emitidos, revocados y suspendidos, a través de una consulta en línea y gratuita por número de serie del certificado, donde se visualice datos como: estado, fecha de emisión, fecha de caducidad, tiempo de vigencia, fecha de revocación, motivo de revocación, fecha de suspensión; estos último tres cuando aplique.

2.3. Tiempo o frecuencia de publicación.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A se responsabiliza por la disponibilidad continua y actualización oportuna de la información publicada en sus repositorios.

Certificado Raíz

El certificado raíz se publicará y permanecerá en la página Web de la Entidad de Certificación SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. durante todo el tiempo en que se estén prestando servicios de certificación digital.

Certificado Subordinada

El certificado de la EC Subordinada se publicará y permanecerá en la página Web de la Entidad de Certificación SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. durante todo el tiempo en que se estén prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A publicará en la página Web, la lista de certificados revocados en los eventos y con la periodicidad diaria o cuando se produzca una revocación o suspensión, y para una consulta rápida la entidad de certificación emite una CRL delta cada 24 horas.

Declaración de Prácticas de Certificación (DPC) y Políticas de Certificación (PC)

Con autorización del Responsable de la Entidad de Certificación de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A y ARCOTEL, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados a ARCOTEL y publicados en la página Web de la Entidad de Certificación de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A junto con la nueva versión. La Auditoría anual validará estos cambios y emitirá el informe de cumplimiento

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	25

2.4. Controles de acceso a los repositorios.

El acceso a la información pública contenida en los repositorios que se encuentran disponibles en la página web de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A será libre y gratuito al público en general y todas las partes confiantes.

Security Data se responsabiliza por:

- La disponibilidad continua de los repositorios
- La integridad de la información publicada
- La autenticidad de los datos

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas a SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.

El acceso a funcionalidades distintas de la consulta pública estará restringido mediante controles de seguridad que incluyen:

- Mecanismos de autenticación
- Control de accesos
- Segregación de funciones
- Monitoreo accesos

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

3.1.2. Necesidad de que los nombres tengan significado.

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

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	26

Los campos del DN referentes a Nombres y Apellidos corresponderán con los datos registrados legalmente del suscriptor, expresados exactamente en el formato que conste en la Cédula de Identidad, tarjeta de residencia, pasaporte u otro medio reconocido en derecho.

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.

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

3.1.3. Anonimato o seudónimo de los Suscriptores.

No 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.

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

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

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

3.1.5. Unicidad de los nombres.

El nombre distinguido (DN) de los certificados emitidos será único para cada suscriptor 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.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	27

3.1.7. Resolución de conflictos relativos a nombres.

Security Data no actúa como árbitro o mediador, ni resuelve ninguna disputa relativa a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, etc. Así mismo, Security Data se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

3.1.8. Comprobación de las facultades de representación.

La comprobación de la representación del solicitante ante Security Data se realizará mediante la comprobación de la documentación de acuerdo al tipo de certificado establecido en la normativa ecuatoriana a través de su ente regulador ARCOTEL.

3.2. Validación inicial de la identidad.

Para la validación de identidad, Security Data aplicará el siguiente Protocolo de Seguridad Escalonado:

1. Validación Biométrica Automatizada: Se realizará una captura del rostro en vivo comparándola contra la base de datos del Registro Civil. El sistema aplicará algoritmos de *Liveness Detection* (detección de vida) para descartar el uso de fotos, videos o máscaras.
2. Validación Reforzada (Fallo Biométrico): Si el sistema biométrico no puede verificar la identidad con el nivel de confianza requerido o superior, el solicitante deberá optar obligatoriamente por:
 - Validación por video: el solicitante deberá realizar una manifestación expresa que permita confirmar su identidad y voluntad respecto a la obtención o renovación del certificado, conforme a los procedimientos internos establecidos por Security Data.
 - Presencialidad: Acudir físicamente a una oficina con su documento original.

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.

Cada Tercero Vinculado es responsable de garantizar la entrega del dispositivo al solicitante de forma segura.

En los otros casos, 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.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	28

3.2.2. Autenticación de la Identidad de la organización.

La Autoridad de Registro solicitará la documentación o información necesaria para garantizar que un nombre o marca pertenece al solicitante o representado de un certificado digital.

La Autoridad de Registro 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 código de identificación fiscal 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, y la identidad será validada de acuerdo a lo indicado en el presente apartado.

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.

3.2.3. Autenticación de la identidad individual.

El Tercero Vinculado verificará de forma fehaciente la identidad de la persona natural identificada en el certificado. Para ello, la persona natural deberá personarse y presentar la cédula de Identidad, pasaporte u otro medio reconocido en derecho que le identifique, y la identidad será validada de acuerdo a lo indicado en el presente apartado.

En caso de que el suscriptor reclame la modificación de los datos de identificación personales a registrar respecto de los del documento de identificación presentado, deberá presentar el correspondiente Certificado del Registro Civil consignando la variación.

El Tercero Vinculado verificará, bien mediante la exhibición de documentación original suficiente, bien con sus propias fuentes de información, fotografía y el resto de datos y atributos a incluir en el certificado (nombre distinguido del certificado), debiendo guardar la documentación acreditativa de la validez de aquellos datos que no puede comprobar por medio de sus propias fuentes de datos.

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.

Autenticación de la Identidad del Tercero Vinculado y de Operadores del Tercero Vinculado.

En la constitución de un nuevo Tercer Vinculado, se realizarán las siguientes acciones:

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	29

Security Data Seguridad en Datos y Firma Digital verificará la existencia de la entidad mediante sus propias fuentes de información.

Un representante autorizado de la organización, deberá firmar un contrato con Security Data Seguridad en Datos y Firma Digital, donde se especificarán los aspectos concretos de la delegación y las responsabilidades de cada agente.

Además, se exigirá al Tercero Vinculado el cumplimiento de lo siguiente respecto de los operadores del Tercero Vinculado:

Verificar y validar la identidad de los nuevos operadores del Tercero Vinculado. El Tercero Vinculado deberá enviar a Security Data Seguridad en Datos y Firma Digital la documentación correspondiente al nuevo operador, así como su autorización a que actúe como operador de Tercero Vinculado.

Asegurar que los operadores de registro hayan recibido formación suficiente para el desempeño de sus funciones, asistiendo como mínimo a una sesión de formación de operador.

Asegurar que la comunicación entre el Tercero Vinculado y Security Data Seguridad en Datos y Firma Digital se realiza de forma segura mediante el uso de certificados digitales de operador. Todos los operadores de Security Data o de Terceros Vinculados deben suscribir obligatoriamente una Declaración de Responsabilidad y Confidencialidad. En este documento, el operador asume responsabilidad civil y penal por la correcta validación de identidad y el manejo de datos personales de acuerdo con la LOPDP. El incumplimiento será causal de revocación inmediata de sus credenciales de acceso.

3.2.4. Información de suscriptor no verificada.

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

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 natural, persona jurídica, cargo o función al que estará asociado el certificado solicitado.

En el caso de certificados emitidos a personas jurídicas, 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 de firma electrónica 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

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	30

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 presente 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 firma electrónica 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.

3.3. Identificación y autenticación en la renovación de claves.

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

Security Data no ofrece el servicio de renovación sin cambio de clave. El suscriptor podrá tramitar la renovación de los certificados de firma electrónica, después de la caducidad del mismo o cuando este así lo requiera, como un proceso nuevo de adquisición de firma electrónica, y la validación se realizará como uno nuevo.

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

El suscriptor podrá tramitar la renovación de los certificados de firma electrónica después de la revocación del mismo, como un proceso nuevo de adquisición de firma electrónica. La validación de identidad se realizará de acuerdo a lo definido en el apartado *Validación Inicial de la Identidad*, como un proceso nuevo.

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 de Security Data Seguridad en Datos y Firma Digital en la Administración de la cuenta.
- b) Cualquier Tercer 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.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	31

4. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO.

4.1. Solicitud de certificados.

4.1.1. Quién puede solicitar un Certificado.

Los requisitos que debe reunir un solicitante dependerán del tipo de certificado solicitado y estarán recogidos en la "Política de Certificación" de cada tipo de certificado concreto.

Security Data solo admite solicitud de emisión de certificado tramitada por una persona física, bajo relación de dependencia (para el caso de personas jurídicas), mayor de edad y con plena capacidad legal de obrar.

4.1.2. Proceso de inscripción y responsabilidades.

El proceso de inscripción para la emisión de certificados electrónicos se inicia a solicitud del interesado, a través de los canales habilitados por la AC, ya sea de manera directa o mediante alguno de los Terceros Vinculados autorizados.

El solicitante deberá contactar a Security Data Seguridad en Datos y Firma Digital para gestionar la solicitud del certificado, ya sea por medio de la página web de la CA, presencialmente o por medio de alguno de los Terceros Vinculados asociados. El Tercero Vinculado proporcionará al solicitante la siguiente información:

- Documentación necesaria a presentar para la tramitación de su solicitud y para verificar la identidad del suscriptor.
- Disponibilidad para realizar el proceso de registro.
- Información sobre el proceso de emisión y revocación, de la custodia de la clave privada, así como de las responsabilidades y las condiciones de uso del certificado y del dispositivo.
- Cómo poder acceder y consultar el presente documento y las Políticas de Certificación.

La Entidad de Certificación registrará la solicitud y procederá a verificar la identidad del solicitante, la integridad y suficiencia de la información y documentación proporcionada, de conformidad con los requisitos establecidos en la "Política de Certificación" de cada tipo de certificado concreto.

Para estos efectos, la documentación proporcionada será validada mediante la consulta en tiempo real a las bases de datos oficiales del Registro Civil y del Servicio de Rentas Internas (SRI), según corresponda. Concluido el proceso de validación, la Entidad de Certificación comunicará al solicitante la aprobación o el rechazo de la solicitud, de acuerdo con los criterios definidos en la presente Declaración de Prácticas de Certificación.

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 DPC. La Entidad de Certificación es responsable de gestionar el

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	32

proceso de inscripción de manera segura, confiable y conforme a los estándares técnicos y regulatorios aplicables.

Validez del certificado de firma electrónica.

De acuerdo al Reglamento de la Ley de comercio electrónico, firmas electrónicas y mensajes de datos (Decreto No.3469):

“La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años, pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en las leyes.”

4.2. Tramitación de solicitud de certificados.

4.2.1. Realización de funciones de Identificación y Autenticación.

Es responsabilidad de la AC y del Tercero Vinculado realizar de forma fehaciente la identificación y autenticación del suscriptor. Este proceso deberá ser realizado previamente a la emisión del certificado.

La validación de la identidad y de la documentación se realizará tanto en modalidad presencial como en línea, ante un operador de la AC o del Tercero Vinculado, aplicando los mismos procedimientos y criterios en ambos casos. La verificación se efectuará mediante la revisión de los documentos de identificación presentados y validación biométrica; de no ser posible esta última, se empleará un mecanismo alternativo de verificación por video, el cual será revisado por el operador para confirmar la identidad del solicitante.

La validación de la documentación se hará de manera presencial u online, el operador de la AC o del Tercero Vinculado realizará la revisión y validación de la información proporcionada. Una vez validada la identidad y los documentos, se procederá con la emisión del certificado de firma electrónica.

4.2.2. Aprobación o rechazo de las solicitudes de certificados.

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

Adicionalmente, también el Solicitante deberá aceptar las condiciones de uso y política de privacidad. Posteriormente, la documentación proporcionada será validada mediante la consulta en tiempo real a las bases de datos oficiales del Registro Civil y del Servicio de Rentas Internas (SRI), según corresponda.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	33

Si la información no es correcta, el Tercero Vinculado denegará la petición, contactando al solicitante para comunicarle el motivo. Si es correcta, se procederá con la emisión de la factura, pago y confirmación de la transacción 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.

Security Data denegará la solicitud en los siguientes casos de seguridad:

- Detección de documentos con vigencia caducada o con indicios de manipulación física/digital.
- Inconsistencia entre los datos del SRI/Registro Civil, u otro ente de control, y la información proporcionada.
- Fallo reiterado en las pruebas de vida (biometría) sin que el usuario acepte la validación por video o presencial.

4.2.3. Tiempo de tramitación de las solicitudes de certificados.

El procesamiento de las solicitudes de certificados de firma electrónica en línea se realizará en un plazo máximo de veinticuatro (24) horas, siempre que el solicitante haya cumplido de manera íntegra con los requisitos establecidos, incluidos, entre otros, la presentación completa y válida de la documentación requerida, la confirmación del pago correspondiente a favor de Security Data y la correcta validación de la identidad.

En caso de detectarse inconsistencias, errores en los archivos proporcionados o información incompleta, el tiempo de gestión podrá extenderse hasta un plazo máximo de 48 horas, contadas a partir de la recepción de la solicitud, mientras el titular subsana las observaciones comunicadas.

Durante todo el proceso, el usuario será informado de manera oportuna y permanente mediante correo electrónico sobre el estado de su solicitud, las causas de cualquier retraso y los pasos necesarios para dar continuidad al trámite hasta su correcta finalización.

El tiempo de procesamiento de solicitudes presencial será de 15 min, si cumple con todos los requisitos y con las condiciones indicadas en este apartado.

4.3. Emisión del certificado.

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

Security Data genera certificados electrónicos, tanto nuevos como renovados, dentro de sistemas con entornos seguros, el cual se encuentra configurado para asegurar una emisión correcta, controlada y conforme a las políticas, prácticas y procedimientos internos, garantizando que cada certificado sea emitido de manera uniforme y de acuerdo con el tipo de certificado electrónico solicitado.

Adicionalmente, Security Data emite certificados de firma en cumplimiento de las leyes, normas y regulaciones que rigen en el territorio ecuatoriano.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	34

Una vez aprobada la solicitud se procederá a la emisión del certificado, que deberá ser entregado de forma segura al suscriptor.

Para la emisión de certificados se realizarán las siguientes acciones:

Para los certificados en soporte hardware:

- El operador de registro o tercero vinculado le hará entrega del DSCF vacío, es decir sin importar el certificado dentro del dispositivo. En caso de que el solicitante aporte su propio dispositivo, éste deberá ser un DSCF entregado anteriormente por Security Data Seguridad en Datos y Firma Digital. Los Terceros Vinculados dispondrán de una lista de dispositivos asignados.
- Activación del dispositivo: En el caso que el solicitante no disponga de un DSCF, se generarán los datos de activación del dispositivo.
- La AC realizará la emisión del certificado en el dispositivo DSCF si el cliente lo desea, caso contrario le enviará a su correo un video tutorial para que el suscriptor pueda importar su certificado en el DSCF.
- Si el dispositivo DSCF es retirado por un tercero debidamente autorizado por el titular, no se realizará la emisión de la firma, en su caso la realizará el suscriptor posteriormente.
- Generación del par de claves: El cliente es responsable de generar la clave asociada al certificado. Una vez completado el proceso de validación y generada la clave, se procederá importando en el dispositivo DSCF.
- La AC proporcionará el procedimiento para el cambio de clave o pin del DSCF.

Para los certificados en Software:

- La AC notificará, mediante correo electrónico al suscriptor, que el certificado se encuentra en el portal del cliente listo para la descarga.
- Posteriormente a que el suscriptor acepte los términos y condiciones y llene el formulario de descarga, la AC enviará a su correo electrónico el Pin de seguridad para la descarga de la firma.
- La AC le enviará al correo electrónico el respaldo de la clave de la firma que colocó el suscriptor al momento de la descarga.

4.3.2. Notificación al suscriptor por parte de la CA de la Emisión del Certificado.

a) En Hardware

- La AC o el Tercer Vinculado le hará entrega del DSCF vacío, es decir sin emitir el certificado dentro del dispositivo, al suscriptor o a la persona autorizada por el solicitante.
- La AC realizará la emisión del certificado en el dispositivo DSCF si el titular lo desea, caso contrario le enviará a su correo un video tutorial para que el suscriptor pueda importar su certificado en el DSCF.

b) En Software

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	35

- La AC notificará mediante correo electrónico al suscriptor, que el certificado se encuentra en el portal del cliente listo para la descarga.

La AC posteriormente a la aprobación de la solicitud, notificará mediante correo electrónico al suscriptor que el certificado de firma electrónica se encuentra en el portal del cliente listo para la descarga.

4.4. Aceptación del certificado.

4.4.1. Conducta que constituye la aceptación del certificado.

El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el suscriptor y Security Data 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.

El documento de aceptación deberá ser firmado electrónicamente una vez que el suscriptor disponga de la correspondiente firma electrónica.

4.4.2. Publicación del Certificado.

Una vez el certificado ha sido generado y aceptado por el suscriptor o firmante, el certificado será publicado inmediatamente en los repositorios de certificados que se consideren necesarios.

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

No se estipula.

4.5. Usos de las 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 DPC y en la Política de Certificación correspondiente.

En caso de que el certificado haya sido comprometido, es decir su clave privada, el suscriptor deberá iniciar un procedimiento de revocación. El certificado de firma electrónica emitido por Security Data al suscriptor, deberá ser utilizado tal y como son suministrados.

Los certificados de firma electrónica presentan las siguientes garantías:

- **Autenticidad:** La información del documento y su firma digital corresponden indubitablemente al suscriptor quien debe estar en todo tiempo en posesión del certificado.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	36

- **Integridad:** La información contenida en el documento electrónico, no ha sido modificada o alterada luego de su firma.
- **No repudio:** La persona que ha firmado electrónicamente no puede negar su autoría.
- **Confidencialidad:** La información contenida ha sido cifrada y por voluntad del emisor, solo se permite que el receptor pueda descifrarla.

El uso de los certificados para fines distintos a los establecidos queda expresamente prohibido.

4.5.2. Uso de la 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 DPC y las Políticas de Certificados correspondientes.

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.

4.5.3. Especificaciones técnicas de los algoritmos y tamaños de clave

SECURITY DATA utilizará algoritmos criptográficos y parámetros que cumplan con estándares internacionales reconocidos y buenas prácticas de seguridad, incluyendo:

- **Algoritmos de clave pública:**
 - RSA con longitud de 2048 bits.
- **Algoritmos de hash:**
 - Funciones hash seguras de SHA-256.
- **Algoritmos de firma electrónica:**
 - RSA con SHA-256.

SECURITY DATA podrá actualizar los algoritmos y tamaños de clave conforme a la evolución de los estándares criptográficos y requisitos regulatorios.

4.5.4. Generación de claves

La generación de pares de claves deberá realizarse en entornos seguros que garanticen:

- La confidencialidad de la clave privada;
- La integridad del proceso de generación;
- La protección contra accesos no autorizados.

Para certificados emitidos bajo infraestructura de certificación:

- Las claves privadas de las Autoridades de Certificación (CA) se generan y resguardan en el HSM.
- Las claves deben generarse según lo especificado en el apartado 6.1. *Generación e instalación de pares de claves.*

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	37

4.6. Renovación del certificado.

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

4.6.1. Circunstancias para la renovación del certificado

No aplica.

4.6.2. Quién puede solicitar la renovación

No aplica.

4.6.3. Tramitación de solicitudes de renovación de certificados

No aplica.

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

No aplica.

4.6.5. Conducta que constituye aceptación de un certificado de renovación

No aplica.

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

No aplica.

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

No aplica.

4.7. Cambio de clave del certificado.

Security Data para el cambio de claves de certificados realiza la emisión de un nuevo certificado.

4.7.1. Circunstancias para la renovación de la clave del certificado.

El proceso de renovación se efectuará del mismo modo que la emisión de un nuevo certificado, ya que el suscriptor tiene en su posesión la llave pública y privada, por tal motivo la entidad de certificación no almacena dicha información y se emite un nuevo certificado y por ende no puede extender la vigencia del certificado sin una nueva emisión de este. Bajo ningún concepto Security Data Seguridad en Datos y Firma Digital ofrece servicios de rekey de certificados.

Se podrá renovar el certificado de firma electrónica bajo las siguientes circunstancias:

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	38

- El certificado ha caducado.
- El certificado ha sido vulnerado.
- Compromiso o sospecha de compromiso de las claves.
- Pérdida o robo de las claves.
- El certificado ha sido revocado.

4.7.2. Quién puede solicitar la certificación de una nueva clave pública.

La renovación del certificado de firma electrónica puede ser solicitado por el titular o un tercero debidamente autorizado y los requisitos que debe reunir dependerán del tipo de certificado solicitado y estarán recogidos en la "Política de Certificación" de cada tipo de certificado concreto.

4.7.3. Procesamiento de solicitudes de Renovación de Claves de certificados.

La solicitud de renovación del certificado de firma electrónica se podrá realizar presencialmente o en línea.

La validación de la identidad puede verificarse mediante la biométrica del rostro del solicitante en atención presencial u online, en caso que no sea posible validar por este medio, el solicitante puede grabar un video que será revisado por un operador de la AC o del Tercero Vinculado, el cual validará la identidad del solicitante por medio de los documentos de identificación. La validación de la documentación se hará de manera presencial u online ante un operador de la AC o del Tercero Vinculado. Una vez validada la identidad y los documentos, se procederá con la emisión del certificado de firma electrónica.

La validación de la identidad se la realizará en base al apartado *Validación Inicial de la Identidad* del presente documento.

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

Security Data notificará al suscriptor sobre la caducidad del certificado por medio de un correo electrónico 30 días antes, previo a la fecha de vencimiento del certificado.

Es potestad del suscriptor renovar o no el certificado de firma.

4.7.5. Conducta que constituye aceptación de un certificado con nueva clave.

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.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	39

El documento de aceptación deberá ser firmado electrónicamente una vez que el suscriptor disponga de la correspondiente firma electrónica.

4.7.6. Publicación del certificado con nueva clave por parte de la CA.

Una vez el certificado ha sido generado y aceptado por el suscriptor o firmante, el certificado podrá ser publicado en los repositorios de certificados publicados en la página web de Security Data.

4.7.7. Notificación de la emisión del certificado por la AC a otras entidades.

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

4.8. Modificación de certificados.

La modificación de un certificado de firma electrónica implica la revocación de la misma y la emisión de una nueva firma.

Aceptación de términos y condiciones para actualización de datos por parte del cliente.

- Generación de un formulario de revocación, el cual será firmado electrónicamente con el certificado vigente del cliente.
- Notificación de la creación del certificado actualizado y de la revocación del certificado anterior mediante correo electrónico al cliente.

4.8.1. Circunstancias para la Modificación del Certificado.

Un certificado de firma electrónica puede ser modificado en las siguientes circunstancias:

- Corrección de errores tipográficos en los datos con los que fue emitida la firma.
- La entidad certificadora, acorde a cambios en la legislación o giros de negocio requiera realizar una actualización de datos en el certificado de firma electrónica del cliente.

4.8.2. Quién puede solicitar la modificación del certificado.

La modificación del certificado puede ser solicitada por el suscriptor o un tercero debidamente autorizado.

4.8.3. Procesamiento de solicitudes de modificación de certificados.

Si el suscriptor detecta algún error en los datos de su firma electrónica, deberá acercarse a las oficinas de la AR o ponerse en contacto con Security Data mediante los canales de atención al cliente, con las respectivas evidencias para la corrección.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	40

El suscriptor deberá revocar el certificado de firma electrónica erróneo, firmando la solicitud con el mismo. A continuación, el operador de la AC corregirá el o los errores y se emitirá el nuevo certificado sin costo para el cliente.

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

La AC notificará mediante correo electrónico al suscriptor que su nuevo certificado se encuentra listo para la descarga desde su perfil de usuario.

4.8.5. Conducta que constituye aceptación del certificado modificado.

El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el suscriptor y Security Data 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.

El documento de aceptación deberá ser firmado electrónicamente una vez que el suscriptor disponga de la correspondiente firma electrónica.

4.8.6. Publicación del certificado modificado por la CA.

Una vez el certificado ha sido generado y aceptado por el suscriptor o firmante, el certificado será publicado inmediatamente en los repositorios de certificados que se consideren necesarios.

4.8.7. Notificación de la emisión del certificado por la CA a otras entidades.

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

4.9. Revocación y suspensión del certificado.

La revocación de un certificado supone la pérdida de validez del mismo, y es irreversible. La suspensión supone la pérdida temporal de validez de un certificado y es reversible.

Las revocaciones y suspensiones tienen efecto desde el momento en que aparecen publicadas en la CRL, las cuales se encuentran detalladas en el punto *Frecuencia de Emisión de CRLs* del presente documento.

4.9.1. Circunstancia de Revocación.

Un certificado podrá ser revocado debido a las siguientes causas:

a) Circunstancias que afectan a la información contenida en el certificado:

- Modificación de alguno de los datos contenidos en el certificado.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	41

- Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
- Pérdida o cambio de la vinculación del firmante con la Organización.

b) Circunstancias que afectan a la seguridad de la clave privada o del certificado:

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

c) Circunstancias que afectan a la seguridad del dispositivo criptográfico:

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado por un tercero a los datos de activación del suscriptor.
- El incumplimiento por parte del suscriptor o firmante de las normas de uso del certificado expuestas en la presente DPC o en el instrumento jurídico vinculante entre Security Data Seguridad en Datos y Firma Digital y el suscriptor.

d) Circunstancias que afectan al suscriptor:

- Finalización de la relación jurídica entre Security Data Seguridad en Datos y Firma Digital y el Suscriptor.
- Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al firmante.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
- Infracción por el suscriptor de sus obligaciones, responsabilidades y garantías, establecidas en el instrumento jurídico correspondiente o en la DPC.
- La incapacidad sobrevenida, total o parcial.
- Por el fallecimiento del suscriptor o firmante: La revocación por fallecimiento surtirá efecto desde la carga del acta de defunción en el portal o su notificación física, invalidando cualquier firma realizada con fecha posterior al deceso según conste en el Registro Civil, independientemente de la fecha de notificación a la AC.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	42

e) Otras circunstancias:

- La suspensión del certificado digital por un período superior al establecido en la DPC.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la DPC.

4.9.2. Quién puede Solicitar la Revocación.

Pueden solicitar la revocación de un certificado:

- El propio suscriptor, que deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.
- El representante legal podrá solicitar la revocación del certificado de cualquier miembro de empresa de su representada.
- La EC que emitió el certificado.
- La ER a través del cual de emitió el certificado.
- Un juez que de acuerdo a la Ley decida revocar el certificado.
- Sucesión: Herederos legítimos en caso de fallecimiento (adjuntando documentación).
- Mandato Judicial: Orden expresa de autoridad competente.
- Cualquier persona podrá solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

Podrán tramitar la revocación del certificado:

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

4.9.3. Procedimientos para la Solicitud de Revocación.

Existen distintas alternativas para el suscriptor a la hora de solicitar la revocación del certificado.

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

Revocación en línea de firmas electrónicas.

La revocación de la firma electrónica se realiza desde el portal del cliente de Security Data, en el cual se encuentra la opción de revocar el certificado del usuario.

La firma electrónica se podrá revocar de las siguientes formas:

- I. **Titular Persona Natural:** El titular, en su calidad de persona natural, podrá solicitar la revocación de su certificado a través del portal, efectuando la firma electrónica correspondiente. La revocación se realizará de manera inmediata, y el ingreso de la

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	43

contraseña asociada a su certificado de firma electrónica, constituye un mecanismo válido de autenticación y manifestación de voluntad:

- El titular accede a su portal.
- Genera la solicitud.
- Ingresa los datos solicitados.

Adicional se le solicita:

- Copia de Cédula.
- En caso de solicitar revocación para personas fallecidas, adicional se debe subir el acta de defunción.

En caso de que el sistema detecte que el titular no dispone de un certificado de firma electrónica activo para autenticarse en línea, se generará la solicitud de revocación y le permitirá descargarlo lleno con la información ingresada, para firmarlo manualmente. Dicho documento debe subirlo en la misma cuenta y esperar la respuesta en el transcurso del día con respecto a la revocación solicitada. El formulario físico deberá ser entregado en las oficinas de la AC para la revocación definitiva, caso contrario el certificado quedará suspendido, o al finalizar un periodo de 90 días el certificado será revocado. Dentro de estos 90 días el solicitante o firmante puede cancelar la suspensión y el procedimiento de revocación.

II. **Titular Persona Jurídica:** El titular, en su calidad de representante legal o miembro de empresa, podrá solicitar la revocación de su certificado a través del portal, efectuando la firma electrónica correspondiente. El sistema solicitará ingresar la contraseña de la firma y pasará a revisión por el departamento encargado, quienes en el transcurso del día darán la respuesta con respecto a la revocación, el ingreso de la contraseña asociada a su certificado de firma electrónica, constituye un mecanismo válido de autenticación y manifestación de voluntad:

- El titular accede a su portal.
- Genera la solicitud.
- Ingresa los datos solicitados.

Adicional se le solicita:

- Copia de Cedula del solicitante.
- Nombramiento Vigente o documento equivalente.
- Para el caso de personas fallecidas, se debe subir el acta de defunción.

En caso de que el sistema detecte que el titular no dispone de un certificado de firma electrónica activo para autenticarse en línea, se generará la solicitud de revocación y le permitirá descargarlo lleno con la información ingresada, para firmarlo manualmente. Dicho documento debe subirlo en la misma cuenta y esperar la respuesta en el transcurso del día con respecto a la revocación solicitada. El formulario físico deberá ser entregado en las oficinas de la AC para la revocación definitiva caso contrario el certificado quedará suspendido, o al finalizar un periodo de 90 días el certificado será revocado. Dentro de estos 90 días el solicitante o firmante puede cancelar la suspensión y el procedimiento de revocación.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	44

- III. **Revocación por tercero:** Un tercero podrá instar la revocación de un certificado ajeno, únicamente cuando acredite competencia legal o interés legítimo. El solicitante deberá:
- Ingresar a su portal personal, debidamente autenticado.
 - Generar la solicitud, ingresando los datos de la persona titular de la firma a revocar y los datos del solicitante.

Adicional se le solicita:

- a. Personas Natural
 - Copia de Cédula del solicitante.
 - Para el caso de personas fallecidas, se debe subir el acta de defunción.
- b. Personas Jurídicas
 - Copia de Cedula del solicitante.
 - Nombramiento Vigente o documento equivalente.
 - Para el caso de personas fallecidas, se debe subir el acta de defunción.

En caso de que el sistema detecte que el solicitante no dispone de un certificado de firma electrónica activo para autenticarse en línea, se generará la solicitud de revocación y le permitirá descargarlo lleno con la información ingresada para firmarlo manualmente. Dicho documento debe subirlo en la misma cuenta y esperar la respuesta en el transcurso del día con respecto a la revocación solicitada. Toda solicitud de tercero quedará en estado pendiente, y el certificado en suspensión cautelar hasta que el departamento de validación de Security Data confirme la vigencia de los documentos.

La revocación definitiva ocurrirá solo tras la entrega física del formulario o tras cumplirse el plazo de 90 días de suspensión, sin que el titular haya solicitado la reactivación.

Revocación presencial en oficinas.

Si se asiste personalmente, el suscriptor o firmante quedará autenticado mediante su cédula de identidad o pasaporte y se podrá proceder a la revocación inmediata del certificado, posterior al llenado de la solicitud de revocación y entregado al operador de la autoridad de registro, en caso de suspensión, el suscriptor puede solicitar previa validación de datos de la AC.

Si se comunica telefónicamente al 02-3922169/04-3922169, el suscriptor recibirá información para realizar el proceso de revocación del certificado y no se iniciará con el proceso hasta que la solicitud sea enviada por WhatsApp o al correo electrónico.

Si lo hace vía correo electrónico a o al WhatsApp 0986442122, el suscriptor debe enviar la copia del documento de identidad y el formulario de revocación, en caso de que la solicitud de revocación se encuentre firmada electrónicamente se procede con la revocación definitiva, caso contrario el certificado quedará suspendido y el formulario físico deberá ser entregado en las oficinas de la AC para la revocación definitiva, o al finalizar un periodo de 90 días el certificado será revocado. Dentro de estos 90 días el solicitante o firmante puede cancelar la suspensión y el procedimiento de revocación.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	45

Security Data verificará de forma estricta la competencia legal del tercero solicitante previo a cualquier acción de revocación:

1. No se procederá con la revocación solicitada por un tercero si este no acredita fehacientemente su capacidad legal (v.gr. Nombramiento vigente de Representante Legal, Poder Especial, o Documento Judicial pertinente) que lo faculte expresamente para actuar sobre el certificado del titular. La ausencia de competencia legal comprobada será causal de rechazo inmediato de la solicitud.
2. El tercero que, mediante el uso de documentación falsa, desactualizada o actuando de forma maliciosa, induzca a error a la AC para revocar un certificado y causar perjuicio al titular o a la organización, asumirá de forma exclusiva la responsabilidad civil y penal derivada de dicho acto.
3. Security Data actúa como ejecutor de buena fe tras la validación administrativa de la documentación presentada. Una vez verificada la competencia legal aparente, conforme a los registros oficiales (Registro Mercantil, portal de la Superintendencia de Compañías, etc.), la AC procederá con la revocación, quedando exenta de responsabilidad por conflictos internos o disputas administrativas entre el tercero y el titular del certificado.

4.9.4. Plazo de gracia para la solicitud de Revocación.

No se estipula un periodo de gracia para las solicitudes de revocación. El proceso de revocación se iniciará inmediatamente después de la recepción de dicha solicitud.

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

4.9.5. Plazo en el que la CA debe tramitar la solicitud de Revocación.

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

4.9.6. Requisito de comprobación de Revocación para las Partes que Confían.

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.

4.9.7. Frecuencia de Emisión de CRLs.

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

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

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	46

4.9.8. Latencia máxima para CRL.

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

4.9.9. Disponibilidad de comprobación de estado/revocación en línea

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

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

4.9.10. Requisitos de Comprobación de Revocación en Línea.

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

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

4.9.11. Otras formas de anuncios de revocación disponibles.

No es aplicable.

4.9.12. Requisitos especiales en materia de Compromiso de Claves.

No es aplicable.

4.9.13. Circunstancias de Suspensión.

Security Data Seguridad en Datos y Firma Digital podrá suspender un certificado en los casos siguientes:

- Si se sospecha el compromiso de una clave, hasta que este hecho sea confirmado o desmentido.
- Si el suscriptor ha incurrido en falta de pago de su certificado.
- Si no disponen de toda la información necesaria para determinar la revocación de un certificado.
- Sea dispuesto por el ARCOTEL, de conformidad en lo previsto en la ley de Comercio electrónico, firmas electrónicas y mensajes de datos.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	47

- Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado.
- Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

4.9.14. Quién puede Solicitar la Suspensión.

Solamente podrán realizar la suspensión del certificado:

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

4.9.15. Procedimiento para solicitud de suspensión.

Para el procedimiento de suspensión de certificado, se seguirá lo indicado en el apartado *Procedimiento para la Solicitud de Revocación* del presente apartado.

4.9.16. Límites del Periodo de Suspensión.

Bajo ningún concepto Security Data Seguridad en Datos y Firma Digital realiza copias de los certificados en caso de caducidad, revocación o suspensión. El cliente será el único ente autorizado para el levantamiento de la suspensión, de acuerdo con el criterio del suscriptor, y el mismo no podrá ser delegada a una tercera persona.

Una vez realizada la suspensión, el número de serie único del certificado pasa al listado de CRL's en estado de suspendido, siendo el suscriptor el único quien puede levantar la suspensión, y Security Data ejecutará los procesos necesarios para quitar el número de serie del certificado del suscriptor de las CRL's, y en caso de que el certificado haya expirado o ya no se encuentre vigente, se emitirá uno nuevo.

Un certificado electrónico podrá mantenerse por 90 días en estado de suspensión. Transcurrido dicho plazo sin que el suscriptor haya solicitado o logrado el levantamiento de la suspensión, la Entidad de Certificación procederá a la revocación definitiva del certificado.

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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	48

Las CRL se las puede descargar dentro de la página oficial <https://www.securitydata.net.ec/firma-electronica-en-ecuador/> en la pestaña Firma Electrónica, Soporte y Consultas opción de “Caducidad de Firma y CRL” URL: <https://consultacertificados.securitydata.net.ec/app-consulta-certificados/#/consultarCert>

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

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

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

Parámetros de emisión de la CRL.

Las listas de certificados de revocación (CRL) son firmadas por la CA Raíz con un algoritmo de firma sha256RSA, las cuales tiene una vigencia de un día posterior a su actualización.

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.

No es aplicable.

4.11. Fin de la suscripción.

Todos los certificados emitidos incorporan de manera obligatoria la fecha de emisión y la fecha de expiración, las cuales constan explícitamente dentro de la estructura del certificado digital. Estas fechas permiten que, una vez alcanzado el plazo de validez definido, el certificado cambie automáticamente su estado a “Caducado”, garantizando así el cierre adecuado de su ciclo de vida sin intervención manual.

Adicionalmente, la caducidad del certificado es verificable directamente en el propio certificado mediante la validación con herramientas.

La suscripción finalizará en el momento de expiración o revocación del certificado.

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	49

4.12. Custodia y recuperación de claves.

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

Security Data no almacena, ni tiene la posibilidad de almacenar la clave privada de los suscriptores.

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

La CA limita su función a emitir y gestionar certificados y su estado (vigencia, revocación), sin intervenir en la generación/gestión de claves de sesión.

Cualquier solicitud de recuperación de claves de sesión será rechazada, informando al solicitante que el servicio no forma parte del esquema de certificación.

5. CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIÓN.

5.1. Controles físicos.

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

La política de seguridad física y del entorno aplicable a los servicios de generación de certificados ofrece protección frente:

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

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

5.1.1. Ubicación del sitio y construcción.

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

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	50

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

5.1.2. Acceso Físico.

El acceso físico a las dependencias de la Entidad Acreditada donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo. Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables, así como Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

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

5.1.3. Energía y Aire Acondicionado.

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

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

5.1.4. Exposiciones al Agua.

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

5.1.5. Protección y Prevención de Incendios.

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

5.1.6. Almacenamiento de medios.

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

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

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	51

5.1.7. Eliminación de residuos.

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

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

5.1.8. Copia de Seguridad externa.

Se establecen respaldos diarios de la información.

5.2. Controles de procedimiento.

5.2.1. Roles de Confianza.

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

- Administrador del sistema PKI: quien se encargará de velar por el cumplimiento de las acciones tecnológicas implementadas para la continuidad operativa, gestionar recursos, políticas, normas y procedimientos.
- Operador del Sistema PKI: asesorará al encargado de seguridad en materias relativas a la seguridad de los activos de información, además será el responsable de la gestión del día a día del sistema (Monitorización, backup, recovery, etc).
- Secretario Técnico (encargado de Infraestructura): asesorará en forma permanente y cercana a las distintas áreas de la Empresa en temas relacionados a la segregación de funciones. Coordinar la respuesta ante incidentes que afecten la segregación de funciones.
- Área de Legal: velará por que la Declaración de Prácticas de Certificación (DPC) y demás documentos normativos aplicables a la AC, estén acorde a la legislación nacional vigente y a los entes reguladores y porque las Políticas de Certificación PC estén constante actualización por la función de la empresa.
- Auditor Interno: Revisará la planificación periódica de auditorías al sistema de certificación y velará por el cumplimiento de las auditorías y que los hallazgos encontrados sean mitigados. Además, será el autorizado a acceder a los logs del sistema y verificar los procedimientos que se realizan sobre el mismo.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	52

- Operador de AC - Operador de Certificación: Responsables de activar las claves de la AC en el entorno Online, o de los procesos de firma de certificados y CRL's en el entorno Root Offline.
- Operador de Tercero Vinculado: Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final.

5.2.2. Número de personas necesarias por tarea.

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

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

5.2.3. Identificación y autenticación por cada rol.

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

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

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

5.2.4. Funciones que requieren separación de funciones.

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

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

5.3. Controles de personal.

5.3.1. Requisitos sobre la Cualificación, Experiencia y Conocimientos Profesionales.

Todo el personal de la AC cuenta con la formación académica, experiencia profesional y capacitación específica necesarias para desempeñar de manera competente las funciones que le han sido asignadas conforme a su rol.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	53

Asimismo, todo el personal tiene firmado un contrato laboral que incluye cláusulas de confidencialidad, así como un acuerdo adicional de no divulgación (NDA), a fin de garantizar la protección de la información sensible y evitar su exposición o uso indebido.

El personal que ocupa puestos de confianza declara estar libre de conflictos de interés que puedan afectar la correcta ejecución de sus funciones y comprometer la imparcialidad, integridad o seguridad de las operaciones de la AC.

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

5.3.2. Procedimiento de verificación de Antecedentes.

Security Data mantiene procedimientos documentados para la verificación de datos personales, laborales y de antecedentes del personal que aspire a ser contratado, independientemente de que desempeñe o no un rol de confianza.

De manera general, los métodos de verificación incluyen la validación de identidad, la revisión del historial laboral y académico, la verificación de referencias profesionales y la consulta de antecedentes judiciales, utilizando fuentes oficiales y mecanismos confiables.

5.3.3. Requisitos de Formación.

Security Data define en los perfiles y descriptivos de cargo los requisitos de formación y competencias necesarias para cada uno de los cargos establecidos dentro de la AC.

Asimismo, todo el personal de la AC recibe capacitación continua en materia de seguridad de la información, con el objetivo de garantizar el cumplimiento de las políticas internas, la normativa vigente y las mejores prácticas del sector además de, realizar los cursos necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada operador.

5.3.4. Frecuencia y requisitos de reentrenamiento.

Security Data imparte las capacitaciones necesarias a sus colaboradores, al menos una vez al año y cuando se implementan modificaciones significativas en el proceso de emisión de certificados digitales, asegurando que el personal mantenga actualizados sus conocimientos y competencias.

5.3.5. Frecuencia y Secuencia de Rotación de Tareas.

No se encuentra estipulado.

5.3.6. Sanciones por acciones No Autorizadas.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	54

Security Data cuenta con una política de Ejecución de Sanciones que establece las medidas disciplinarias aplicables a los colaboradores de la AC en caso de realizar acciones no autorizadas, indebidas o contrarias a las políticas y procedimientos establecidos.

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

Independientemente de las sanciones laborales, Security Data se reserva el derecho de ejercer acciones legales de repetición contra cualquier empleado o tercero vinculado que, mediante dolo o negligencia grave, cause un perjuicio económico o reputacional a la AC por el incumplimiento de los protocolos descritos en esta DPC.

5.3.7. Requisitos de contratista independiente.

Los terceros contratados por Security Data deberán firmar un acuerdo de no divulgación (NDA), así como un contrato de prestación de servicios que incluya de manera expresa una cláusula de confidencialidad, garantizando la protección de la información a la que tengan acceso durante la relación contractual.

El personal contratado para fines específicos dentro de las operaciones de la AC, será evaluado respecto de sus antecedentes penales, conocimiento, formación académica y experiencia necesarios para el cargo.

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

5.3.8. Documentación suinistrada al Personal.

A todo el personal incorporado dentro de Security Data Seguridad en Datos y Firma Digital se le proporciona toda la documentación requerida para el desempeño de sus funciones, estos son políticas, procedimientos y formatos de todos los procesos de la AC, teniendo en cuenta la siguiente documentación:

- Reglamento Interno de Seguridad y Salud del Trabajo.
- Reglamento Interno.
- Manual de Usuario de Seguridad de la Información.
- Organización de la Seguridad de la información.

5.4. Procedimientos de registro de auditoría.

5.4.1. Tipos de Eventos Registrados.

SECURITY DATA registra y guarda los logs de todos los eventos relativos al sistema de seguridad de la AC. Estos incluyen los siguientes eventos:

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	55

- 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.
- 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 del procesamiento de Registro.

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 del registro de auditoría.

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 Autoridad de Certificación.

Los dispositivos son manejados en todo momento por personal autorizado.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	56

5.4.5. Procedimientos de copia de seguridad del Registro 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.

La AC tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs. Se realizan copias diarias incrementales y completas semanales.

5.4.6. Sistema de recopilación de Auditorías.

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 al sujeto causante del evento.

La AC dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

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. Evaluaciones de Vulnerabilidades.

Security Data realiza un análisis constante de las vulnerabilidades los cuales son tratados y subsanados de forma inmediata. Además, se realiza una revisión anual de discrepancias en la información de los logs y actividades sospechosas.

5.5. Archivo de registro.

5.5.1. Tipo de registros Archivados.

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

- Todos los datos de la auditoría.
- Todos los datos relativos a los certificados, incluyendo los contratos con los suscriptores y los datos relativos a su identificación.
- Solicitudes de emisión y revocación de certificados.
- Todos los certificados emitidos o publicados.
- CRL's emitidas o registros del estado de los certificados generados.
- La documentación requerida por los auditores.
- Las comunicaciones entre los elementos de la PKI.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	57

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

5.5.2. Periodo de Conservación de los datos archivados.

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

Los contratos con los suscriptores y cualquier información relativa a la identificación y autenticación del suscriptor serán conservados durante al menos 10 años o el periodo que establezca la legislación vigente.

5.5.3. Protección del Archivo.

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

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

5.5.4. Procedimientos de Copia de Seguridad del Archivo.

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

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

Los registros están fechados con una fuente fiable. Dentro de la documentación técnica y de configuración de la AC, se tiene establecido un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

5.5.6. Sistema de recopilación de archivos.

No estipulado.

5.5.7. Procedimientos para obtener y verificar información de archivo.

Los eventos registrados se encuentran protegidos frente a alteraciones o manipulaciones no autorizadas. El acceso a los archivos que contienen dichos registros está estrictamente restringido a personal debidamente autorizado, quien es responsable de realizar las verificaciones de integridad correspondientes para garantizar su fiabilidad y trazabilidad.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	58

Durante la auditoria requerida por esta DPC, el auditor verificará la integridad de la información archivada. La AC proporcionará la información y los medios al auditor para poder verificar la información archivada.

5.6. Cambio de clave.

AC Raíz.

Antes de que el certificado de la AC Raíz expire se realizará un cambio de claves (rekeying) y, en su caso, se introducirán cambios en el contenido del certificado que se ajusten mejor a la legislación vigente y la realidad de Security Data Seguridad en Datos y Firma Digital y del mercado. La AC antigua y su clave privada sólo se usarán para la firma de CRL's mientras existan certificados activos emitidos por la AC antigua. Se generará una nueva AC con una clave privada nueva.

La documentación técnica y de seguridad de la AC detalla el proceso de cambio de claves de la AC. Las claves de los certificados emitidos por AC Raíz dejarán de tener validez en el mismo momento en que lo haga su certificado autofirmado. Una vez expirada la AC Raíz generará un nuevo par de claves que auto firma para generar el nuevo certificado raíz. El cambio de claves no es una operación recurrente de una autoridad de Certificación y debe ser planeada conforme a las condiciones técnicas y regulatorias que se encuentren vigentes.

AC Subordinada.

En el caso de las AC subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves. Sólo cuando se realice el cambio se aplicará lo descrito en el apartado AC Raíz de la presente sección.

5.7. Compromiso y recuperación ante desastres.

5.7.1. Procedimientos de manejo de incidentes y compromisos.

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

5.7.2. Los recursos informáticos, el software y/o los datos están dañados.

En el caso de que tuviera lugar un incidente que alterará o corrompiera tanto recursos de hardware, software como datos, Security Data Seguridad en Datos y Firma Digital procederá según lo estipulado en el procedimiento de Gestión de Eventos e Incidentes de Seguridad de la Información.

5.7.3. Procedimientos de compromiso de la Clave Privada de la entidad.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	59

Se considera el compromiso o sospecha de su clave privada como un incidente y será atendido como un incidente mayor de la prestación de los servicios de certificación digital, por lo que se seguirá los procedimientos internos establecidos para la gestión de incidentes.

En caso de compromiso de la clave privada de la AC, Security Data Seguridad en Datos y Firma Digital:

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

Luego de haber informado por los medios pertinentes, Security Data realizará el proceso de emisión de nuevas claves de la CA, según lo estipulado en los procedimientos internos.

5.7.4. Capacidades de continuidad del negocio después de un desastre.

Para la continuidad del negocio, Security Data tiene definido que:

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

5.8. Terminación de CA o RA.

Autoridad de Certificación.

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

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

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	60

Autoridad de Registro.

Ante el cese de una autoridad de registro de un colectivo específico, Security Data Seguridad en Datos y Firma Digital:

- Dejará de emitir y renovar certificados de esa AR.
- Revocará los certificados de operador de esa AR.
- Revocará los certificados de suscriptor emitidos por esa AR, salvo que expresamente se decida lo contrario.

6. CONTROLES TÉCNICOS DE SEGURIDAD.

6.1. Generación e instalación de pares de claves.

6.1.1. Generación de pares de claves.

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

En hardware (soporte físico).

La generación de la clave de las ACs se realiza, de acuerdo con el proceso documentado de ceremonia de claves, dentro de la sala de seguridad de la Entidad Acreditada, en dispositivos criptográficos hardware (HSM), por personal adecuado según los roles de confianza y, al menos con un control dual y testigos de Security Data Seguridad en Datos y Firma Digital, de la organización titular de la AC y del auditor externo.

Para los certificados de entidad final, el par de claves será creado en el mismo dispositivo utilizando el sistema proporcionado por la AR. Este proceso está vinculado de forma segura al proceso de generación del certificado, garantizando la confidencialidad de la clave privada durante el proceso de generación y la complementariedad entre los datos de creación y verificación de firma.

En software.

El suscriptor recibirá un correo electrónico para conectarse al servicio de generación de certificados de Security Data Seguridad en Datos y Firma Digital. El suscriptor generará el par de claves en su sistema y enviará la clave pública a la AC en formato PKCS10 u otro equivalente.

En otros casos, la generación de claves del suscriptor se realizará en dispositivos que aseguran razonablemente que la clave privada será protegida por el suscriptor contra la utilización por otros, bien por medios físicos, bien estableciendo el suscriptor los controles y medidas de seguridad adecuadas.

6.1.2. Entrega de la Clave Privada al Suscriptor.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	61

En hardware (soporte físico).

La clave privada será entregada junto al certificado en el dispositivo de creación de firma, cuando el suscriptor desee que sea importado dentro del dispositivo DSCF; no obstante, aun cuando la importación no se haya realizado, tanto la clave privada como el dispositivo permanecerán bajo responsabilidad y custodia del suscriptor. El Tercero Vinculado será responsable de garantizar la entrega del dispositivo al suscriptor e indicar el cambio de clave del dispositivo físico, asegurándose así que éste último está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

El dispositivo criptográfico utiliza una clave de activación para el acceso a las claves privadas.

En software.

El suscriptor generará el par de claves directamente en formato .p12.

6.1.3. Entrega de la Clave Pública al Emisor del Certificado.

El envío de la clave pública a la AC para la generación del certificado se realiza mediante un formato estándar preferiblemente en formato PKCS#10 o X.509 autofirmado, la raíz y subordinado están publicados en la página web de Security Data y del cliente acorde al apartado anterior ya que es un conjunto de claves públicas y privadas.

6.1.4. Entrega de la Clave Pública de la AC a partes confiables.

El certificado de las ACs de la cadena de certificación está a disposición de los usuarios en la página web de Security Data Seguridad en Datos y Firma Digital.

6.1.5. Tamaños de clave.

El tamaño de la clave pública y privada que utiliza la AC raíz y Subordinada es de 4096 bits. El tamaño de las claves del usuario final es de 2048 bits.

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

La AC establece procedimientos formales para la emisión de certificados electrónicos, garantizando el uso de algoritmos y longitudes de clave conformes con estándares criptográficos reconocidos y con la normativa vigente.

La generación de parámetros criptográficos y de pares de claves se realiza en entornos seguros y controlados, utilizando módulos criptográficos certificados, tales como Hardware Security Modules (HSM), bajo estrictos controles de acceso físico y lógico, y aplicando el principio de segregación de funciones.

La calidad criptográfica del material de claves y de la clave pública recibida se verificará mediante controles automáticos por parte del Software y hardware PKI, de igual forma se almacenarán los logs de creación y emisión de certificados.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	62

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

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

Los usos admitidos de la clave para cada certificado están definidos en las Políticas de Certificados correspondiente a cada tipo de certificado.

6.2. Protección de claves privadas e ingeniería de módulos criptográficos.

6.2.1. Estándares para los Módulos Criptográficos.

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

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

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

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

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

6.2.3. Custodia de la Clave Privada.

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

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

6.2.4. Copia de Seguridad de la Clave Privada de la AC.

Existen unos dispositivos que permiten la restauración de la clave privada de la AC, que son almacenados de forma segura y sólo accesibles por personal autorizado según los roles de confianza, usando al menos un control dual en un medio físico seguro.

Las claves de la AC Raíz se pueden restaurar de acuerdo con lo indicado en el procedimiento para garantizar el cumplimiento de las Operaciones de la AC.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	63

Para el procedimiento de respaldo de claves privadas de la AC se cargará el software de seguridad del HSM en el dispositivo criptográfico y se realizan las configuraciones necesarias para la disponibilidad de las claves privadas y se inician los servicios en un servidor sin acceso a internet.

6.2.5. Archivado de Claves Privadas.

La AC no archivará, ni almacenará la clave privada de firma de certificados después de la expiración del periodo de validez de la misma.

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

Las claves privadas de los suscriptores pueden ser archivadas por ellos mismos, mediante la conservación del certificado en formato PKCS#12, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la clave pública, siempre que el dispositivo de custodia permita la operación. La AC no almacenará los certificados del suscriptor, los mismos serán eliminados una vez se hayan enviado por el mecanismo seguro.

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

Existe un procedimiento interno de ceremonia de claves de la EC, en donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

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

6.2.7. Almacenamiento de clave privada en el módulo criptográfico.

Las claves privadas asociadas a la AC son generadas y almacenadas exclusivamente dentro de módulos criptográficos seguros (HSM), certificados con la norma FIPS 140-2 nivel 3.

El almacenamiento de la clave privada se realiza de forma que dicha clave no sea exportable ni accesible en texto claro, garantizando su confidencialidad, integridad y disponibilidad durante todo su ciclo de vida. En ningún caso la clave privada será revelada, transferida o puesta a disposición de personas no autorizadas.

El acceso al módulo criptográfico se encuentra estrictamente controlado mediante mecanismos de autenticación fuerte, segregación de funciones y controles de doble custodia, limitándose exclusivamente al personal autorizado y debidamente habilitado conforme a lo establecido en la DPC y en la presente DPS.

La Autoridad de Certificación implementa controles de auditoría y monitoreo permanente sobre el uso del módulo criptográfico, manteniendo registros trazables de todas las operaciones relacionadas con la gestión de claves privadas.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	64

6.2.8. Método de Activación de la Clave Privada.

Las claves de la EC Raíz se activan por un proceso que requiere la utilización simultánea de 3 ACs (tarjetas). Las claves de las EC Subordinadas se activan por un proceso que requiere la utilización de 1 de 2 dispositivos criptográficos (tarjetas).

El acceso a la clave privada del suscriptor se realiza por medio de un PIN o contraseña o de ser el caso por medio de la huella digital. El dispositivo con pin tiene un sistema de protección contra intentos de acceso que lo bloquean cuando se introducen más de seis veces un código de acceso erróneo.

6.2.9. Método de Desactivación de la Clave Privada.

La clave privada del suscriptor de certificados con DSCF quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura. Para claves en software, la desactivación ocurre al cerrar la sesión de la aplicación de firma. La AC no será responsable de ningún uso realizado si el suscriptor deja el dispositivo conectado o la sesión abierta en su equipo informático.

Para la desactivación de la clave privada de la CA Raíz y CA Subordinada se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

6.2.10. Método de Destrucción de la Clave Privada.

El método de destrucción se debe regir de acuerdo con lo indicado en Procedimiento para Eliminación de Información y Destrucción de Claves.

Criterios para la destrucción:

- En caso de manipulación no autorizada del dispositivo criptográfico.
- Cuando el dispositivo es reemplazado, se eliminan las claves de la CA del dispositivo.
- Por un funcionamiento incorrecto del software y hardware del dispositivo criptográfico.
- Respaldo y recuperación de la información del dispositivo criptográfico.
- Al final del ciclo de vida del par de claves de la CA, para la eliminación de copias y sus fragmentos.
- En caso de que las claves contenidas en el dispositivo no sirvan para un propósito comercial válido.
- Levantamiento de un nuevo dispositivo criptográfico para su uso.

Security Data utilizará a individuos en roles de confianza para eliminar las claves privadas cuando cumpla con los criterios antes descritos.

6.2.11. Clasificación del módulo criptográfico.

La calificación del Módulo criptográfico deberá cumplir con los requisitos establecidos en la sección *Estándares para los Módulos Criptográficos* del presente documento.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	65

6.3. Otros aspectos de la gestión de pares de claves.

6.3.1. Archivo de la Clave Pública.

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

6.3.2. Periodos operativos de los Certificados y Periodo de uso del Par de Claves.

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

Un certificado no debe ser usado después del periodo de validez del mismo, aunque los terceros que confían puedan usarlo para verificar datos históricos, teniendo en cuenta que no existirá un servicio de verificación en línea válido para ese certificado.

6.4. Datos de activación.

6.4.1. Generación e Instalación de los Datos de Activación.

Los datos de activación son generados en el momento de la generación del certificado en formato PKCS#12.

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

6.4.2. Protección de los Datos de Activación.

Sólo el personal autorizado tiene conocimiento de los datos de activación de las claves privadas de la AC raíz y AC subordinadas.

Para los certificados de entidad final, una vez se ha hecho entrega del dispositivo y de los datos de activación, es responsabilidad del suscriptor de mantener la confidencialidad de estos datos.

6.4.3. Otros aspectos de los datos de activación.

No estipulado.

6.5. Controles de seguridad informática.

La AC emplea sistemas fiables y productos comerciales para ofrecer sus servicios de certificación. Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Security Data Seguridad en Datos y Firma Digital en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	66

- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

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

6.5.1. Requisitos técnicos de seguridad informática.

Cada servidor de la AC incluye las siguientes funcionalidades:

- Control de acceso a los servicios de AC y gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor y la AC y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de la AC.
- Mecanismos de recuperación de claves y del sistema de AC.

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

6.5.2. Clasificación de la Seguridad Informática.

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que, las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

La protección física del entorno está respaldada por las instalaciones mencionadas anteriormente, mientras que la administración del personal es eficiente gracias al reducido grupo de trabajadores que opera en el centro de datos de Security Data Seguridad en Datos y Firma Digital.

6.6. Controles técnicos del ciclo de vida.

6.6.1. Controles de Desarrollo de Sistemas.

La AC realiza el levantamiento y análisis sistemático de los requisitos de seguridad aplicables a todo proyecto de desarrollo o evolución de los sistemas, con el fin de prevenir vulnerabilidades y asegurar la confidencialidad, integridad, disponibilidad de la información y servicios.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	67

La AC mantiene un procedimiento formal de control de cambios para versiones y aplicaciones que introduzcan mejoras de seguridad o corrijan vulnerabilidades detectadas. Todo cambio requiere registro, análisis de riesgos, planificación de pruebas, aprobación previa y, cuando corresponda, plan de rollback.

6.6.2. Controles de Gestión de Seguridad.

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

La AC mantiene un inventario de activos y documentación, establecidos en sus procedimientos internos, para garantizar su uso. Los documentos están catalogados en tres niveles: PÚBLICO, INTERNO y CONFIDENCIAL.

Para la gestión de accesos a los sistemas, la AC realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el acceso al sistema está limitado a las personas autorizadas. En particular:

a) Gestión general de la AC:

- Se dispone de controles basados en firewalls de alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.
- La AC dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso.
- Cada persona tiene asociado su identificador para realizar las operaciones de certificación según su rol.
- El personal de la AC será responsable de sus actos, por ejemplo, por retener logs de eventos.

b) Generación del certificado:

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

c) Gestión de la revocación:

- La revocación se refiere a la pérdida de efectividad de un certificado digital de forma Permanente, la revocación se realizará mediante autenticación fuerte. Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de AC.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	68

d) Estado de la revocación:

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

Adicional, Security Data sigue el enfoque de seguridad de acuerdo a la norma ISO 27001.

6.6.3. Controles de Seguridad del Ciclo de Vida.

Security Data gestiona la seguridad del ciclo de vida de la siguiente manera:

- La AC se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.
- El Hardware criptográfico está construido sobre soportes preparados para evitar cualquier manipulación.
- La AC registra toda la información pertinente del dispositivo para añadir al catálogo de activos de Security Data Seguridad en Datos y Firma Digital, S.A.
- El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.
- Security Data Seguridad en Datos y Firma Digital realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.
- El dispositivo criptográfico solo es manipulado por personal confiable.
- La clave privada de firma de la AC almacenada en el hardware criptográfico se eliminará una vez se haya retirado el dispositivo.
- La AC posee un contrato de mantenimiento del dispositivo para su correcto mantenimiento. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7. Controles de seguridad de la red.

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

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

6.8. Sellado de tiempo.

La AC ofrece también el servicio de sellado de tiempo con la finalidad de proporcionar evidencia confiable de la fecha y hora en que se firmó un documento electrónico, vinculando de forma segura dicha información temporal a un conjunto específico de datos, garantizando su integridad y verificabilidad.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	69

El sellado de tiempo no implica validación alguna sobre el contenido, origen o licitud de los datos sellados, siendo responsabilidad exclusiva del solicitante el uso que se haga del servicio. Las condiciones específicas del servicio de sellado de tiempo se encuentran detalladas en la Declaración de Prácticas de Sellado de Tiempo correspondiente.

7. PERFILES DE LOS CERTIFICADOS CRL Y OCSP.

7.1. Perfil de los certificados.

El perfil de los certificados se encuentra en las Políticas de Certificados (PC) correspondientes a cada tipo de certificado y son coherentes con lo dispuesto en las normas siguientes:

- ETSI TS 101 862 conocida como "European profile for Qualified Certificates"
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
- RFC 3739 "Qualified Certificates Profile"
- Resolución ARCOTEL-2024-0176 "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS".

Tipos de Certificados.

Los tipos de certificado que emite Security data son:

- Persona Natural.
- Representante Legal.
- Miembro de Empresa o Empleado con Relación de Dependencia.
- Sello electrónico.

La Política de los Certificados se puede encontrar en las siguientes URL:

Persona Natural: <https://www.securitydata.net.ec/normativas/pcnatural.pdf>

Representante Legal: <https://www.securitydata.net.ec/normativas/pcrlegal.pdf>

Miembro de Empresa: <https://www.securitydata.net.ec/normativas/pcmempresa.pdf>

Sello Electrónico: <https://www.securitydata.net.ec/normativas/pcselloelectronico.pdf>

Sello de Tiempo: <https://www.securitydata.net.ec/normativas/pcsellootempo.pdf>

La vigencia del par de claves será de acuerdo con lo solicitado por el suscriptor basado en los siguientes parámetros:

- Para Personas Naturales: desde 1 día y 1 mes, exclusivamente sin RUC, y desde 1 hasta 5 años.
- Para Personas Jurídicas: lo máximo permitido por el nombramiento del representante legal que puede variar entre 1 a 5 años.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	70

Certificados Raíces.

- Certificado raíz CA
https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/cacert.cer
- Certificado raíz subordinada SUBCA-1
https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SUBCA-1.cer
- Certificado raíz CA-2
https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SECDATA-CA-2.cer
- Certificado raíz subordinada SUBCA-2
https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SECDATA-SUBCA2.cer

Certificados Persona Jurídica.

Los Certificados Corporativos son certificados reconocidos de firma electrónica cuyo suscriptor es una Corporación (ya sea una empresa, una organización, o una Administración Pública):

- Certificados Corporativos de Representante Legal: Son certificados reconocidos de persona natural que identifican al suscriptor como una corporación y al firmante como representante legal de dicha corporación.
- Certificados Corporativos de Miembro de Empresa: Son certificados reconocidos de persona natural que identifican al suscriptor como Corporación y al firmante como vinculado a esa corporación como empleado.

Certificados Persona Natural.

Certificados Persona Natural: Son certificados reconocidos de persona natural que identifican al suscriptor como una persona natural pudiendo ser usado este certificado para temas tributarios, legales y personales.

Tipos de Soporte.

Los Certificados de Persona Natural o Jurídica pueden generarse en dos tipos de soporte hardware, software:

a) Dispositivo Seguro de Creación de Firma (DSCF).

Las claves privadas de los certificados emitidos en soporte hardware se generan y almacenan en un "Dispositivo Seguro de Creación de Firma (DSCF)", como una Tarjeta Inteligente o un DSCF criptográfico. Los DSCF proporcionados por Security Data Seguridad en Datos y Firma Digital S.A son certificados FIPS.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	71

Por lo tanto, la utilización de Certificados de Miembro de Empresa con DSCF permite realizar firmas electrónicas con alta seguridad.

Las claves de certificados generadas en DSCF no pueden ser copiadas de ninguna manera, por lo que, si se pierde o se estropea el dispositivo, será necesario realizar un nuevo proceso de emisión de certificado.

Para la activación del DSCF será necesario ingresar el código de activación (PIN) proporcionado por el fabricante. Por razones de seguridad, se recomienda al titular del dispositivo, tanto de manera presencial como mediante correo electrónico, que proceda al cambio inmediato de dicha contraseña, estableciendo una credencial personal y confidencial.

A partir de la modificación del PIN inicial, el usuario será el único responsable de la administración, custodia y uso de su nueva contraseña, debiendo adoptar las medidas necesarias para su adecuada protección y para prevenir accesos no autorizados al dispositivo.

Si se introduce la contraseña o PIN cinco veces seguidas de manera incorrecta, el dispositivo quedará bloqueado, y por lo tanto inservible. Para proceder al desbloqueo se deberá acercarse al Tercero Vinculado donde adquirió el certificado con el dispositivo bloqueado o enviarlo a la misma, en donde se realizará el desbloqueo, o lo puede tramitar de manera remota. El PIN es secreto y personal para el usuario, se le entregará un PIN inicial el que debe ser modificado posteriormente por el usuario utilizando las aplicaciones correspondientes.

Distribución de DSCF.

Los DSCF distribuidos por Security Data, previa validación de identidad del suscriptor, son entregados de tres formas:

- Directamente al suscriptor.
- A una tercera persona debidamente autorizada por el suscriptor.
- Envío a domicilio.

b) Soporte en Software.

Este servicio permite al usuario, después de haber realizado la solicitud y siendo aprobada por la Entidad Certificadora y luego de haber recibido el correo de generación del certificado, acceder al portal de Security Data y poder generar el certificado digital con sus llaves públicas y privadas, almacenándose en el CAPI de Windows de la PC del cliente o como archivo con extensión .p12/.pfx en la misma, siendo el uso de estos certificados para firmar y encriptar documentos y para correo cifrado.

Perfil del Certificado.

El perfil básico a todos los certificados de los suscriptores es el siguiente:

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	72

Tabla 1: Perfil básico de todos los certificados de los suscriptores.

CAMPO DEL CERTIFICADO	NOMBRE	DESCRIPCIÓN
Versión	Número de versión	V3 (Versión del estándar x.509)
Serial Number	Número de serie	Código único con respecto al nombre distinguido del emisor
Signature Algorithm	Algoritmo de firma	Algoritmo de firma sha256RSA
Signature hash algorithm	Algoritmo hash de firma	Sha256
Issuer	Emisor	DN de la CA que emite el certificado
Validity	Validez	Fecha de inicio y fin de validez, tiempo UTC
Subject	Sujeto	Nombre distinguido del suscriptor
Subject Public key info	Clave pública	Clave pública del suscriptor

Los perfiles de los certificados, específicos para cada tipo de certificado otorgado por Security Data, se encuentran establecidos dentro de la PC.

a) CA Raíz Y CA Subordinada.

La cadena de confianza emitida para la infraestructura de clave pública tanto para la CA raíz y CA-subordinada fueron emitidos con algoritmos de cifrado sha256RSA y con un tamaño de clave de 4096 bits.

Tabla 2: Perfil Certificado Raíz – AC

CERTIFICADO RAÍZ - AC (ROOT) - ANEXO 6				
Campo	Contenido	Obligatorio	Crít.	Observaciones OID 1.3.6.1.4.1.37746.1
1. Basic structure				
1.1 Version	3	Sí		El literal "2" corresponde a la versión 3.
1.2 Serial Number	Numero Positivo Hexadecimal 0x41BBD251	Sí		No puede ser un número negativo ni 0.
1.3 Signature Algorithm		Sí		
1.3.1 Identifier	SHA-256 with RSA	Sí		1.2.840.113549.1.1.11
1.3.2 Description	OBJECT IDENTIFIER	Sí		
1.4 Issuer		Sí		
1.4.1 Common Name (CN)	AUTORIDAD DE CERTIFICACION RAIZ CA-2 SECURITY DATA	Sí		OID 2.5.4.3
1.4.2 Country (C)	EC	Sí		OID 2.5.4.6
1.4.3 Organization Name (O)	SECURITY DATA S.A. 2	Sí		OID 2.5.4.10
1.4.5 Organizational Unit (OU)	ENTIDAD DE CERTIFICACION DE INFORMACION	No		OID 2.5.4.11
1.5 Validity		Sí		
1.5.1 Not Before	2019-10-15 16:20:12 ECT	Sí		YYMMDDHHMMSSZ
1.5.2 Not After	2039-10-06 16:20:12 ECT	Sí		YYMMDDHHMMSSZ
1.6 Subject		Sí		

CÓDIGO	SD-ID-PE-09
VERSIÓN	V13
FECHA DE APROBACIÓN	26/03/2026
PÁGINAS	73

1.6.1 Common Name (CN)	AUTORIDAD DE CERTIFICACION RAIZ CA-2 SECURITY DATA	Sí		OID 2.5.4.3
1.6.2 Country (C)	EC	Sí		OID 2.5.4.6
1.6.3 Organization Name(O)	SECURITY DATA S.A. 2	Sí		OID 2.5.4.10
1.6.5 Organizational Unit (OU)	ENTIDAD DE CERTIFICACION DE INFORMACION	No		OID 2.5.4.11
1.7 Subject Public Key Info		Sí		
1.7.1 AlgorithmIdentifier				
1.7.1.1 Algorithm	RsaEncryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2 Parameters		No		
1.7.2 SubjectPublicKey		Sí		
2.1 Authority Key Identifier		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 forma de certificado "AUTOFIRMADO"
2.1.1 Key Identifier		No		Derivado de la clave pública
2.2 Subject Key Identifier		Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1 KeyIdentifier		Sí		
2.3 Key Usage		Sí		OID 2.5.29.15
2.3.1 Digital Signature	True -> Digital Signature			
2.3.2 Content commitment				
2.3.3 Key Encipherment				
2.3.4 Data Encipherment				
2.3.5 Key Agreement				
2.3.6 Key Certificate Signature	True -> Certificate Signing	Sí		
2.3.7 CRL Signature	True -> CRL Signing	Sí		
2.4 Certificate Policies		Sí	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1 Policy Information		Sí		
2.4.1.1 Policy Identifier	1.3.6.1.4.1.37746.1	Sí		Identificador de la política
2.4.1.2 Policy Qualifier ID		Sí		
2.4.1.2.1 CPS Pointer		Sí		
2.4.1.2.2 User Notice		Sí		
2.5 Subject Alternative Names			No	
2.6 Basic Constraints		Sí	Sí	OID 2.5.29.19
2.6.1 Subject type	Subject is a CA	Sí		
2.6.2 Path Length Constraints	None	Sí		

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	74

Tabla 3: Perfil Certificado Subordinado – AC SUB

CERTIFICADO SUBORDINADO - AC SUB - ANEXO 7				
Campo	Contenido	Obligatorio	Crít.	Observaciones OID 1.3.6.1.4.1.OID_Ac.n
1. Basic structure				
1.1 Version	3	Sí		El literal "2" corresponde a la versión 3. X.509 v3
1.2 Serial Number	Numero Positivo Hexadecimal 0x589AE890	Sí		No puede ser un número negativo ni 0.
1.3 Signature Algorithm		Sí		
1.3.1 Identifier	SHA-256 with RSA	Sí		1.2.840.113549.1.1.11
1.3.2 Description	OBJECT IDENTIFIER	Sí		
1.4 Issuer		Sí		
1.4.1 Common Name (CN)	AUTORIDAD DE CERTIFICACION RAIZ CA-2 SECURITY DATA	Sí		OID 2.5.4.3
1.4.2 Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.3 Organization Name (O)	SECURITY DATA S.A. 2	Sí		OID 2.5.4.10
1.4.5 Organizational Unit (OU)	ENTIDAD DE CERTIFICACION DE INFORMACION	No		OID 2.5.4.11
1.5 Validity		Sí		
1.5.1 Not Before	2019-10-15 17:15:57 ECT	Sí		YYMMDDHHMMSSZ
1.5.2 Not After	2039-04-07 17:15:57 ECT	Sí		YYMMDDHHMMSSZ
1.6 Subject		Sí		
1.6.1 Common Name (CN)	AUTORIDAD DE CERTIFICACION SUBCA-2 SECURITY DATA	Sí		OID 2.5.4.3
1.6.2 Country Name(C)	EC	Sí		OID 2.5.4.6
1.6.3 Organization Name (O)	SECURITY DATA S.A. 2	Sí		OID 2.5.4.10
1.6.5 Organizational Unit (OU)	ENTIDAD DE CERTIFICACION DE INFORMACION	No		OID 2.5.4.11
1.7 Subject Public Key Info		Sí		
1.7.1 AlgorithmIdentifier				OID 1.2.840.113549.1.1.1
1.7.1.1 Algorithm	RsaEncryption	Sí		
1.7.1.2 Parameters		No		
1.7.2 SubjectPublicKey		Sí		
2.1 Authority Key Identifier		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 forma de certificado "AUTOFIRMADO"
2.1.1 Key Identifier		No		
2.2 Subject Key Identifier		Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1 KeyIdentifier		Sí		
2.3 Key Usage		Sí		OID 2.5.29.15

2.3.1 Digital Signature	True -> Digital Signature			
2.3.2 Content commitment				
2.3.3 Key Encipherment				
2.3.4 Data Encipherment				
2.3.5 Key Agreement				
2.3.6 Key Certificate Signature	True -> Certificate Signing	Sí		
2.3.7 CRL Signature	True -> CRL Signing	Sí		
2.4 Certificate Policies		Sí	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1 Policy Information		Sí		
2.4.1.1 Policy Identifier	1.3.6.1.4.1.37746.1.9	Sí		Identificador de la política
2.4.1.2 Policy Qualifier ID	(1.3.6.1.5.5.7.2.1)	Sí		
2.4.1.2.1 CPS Pointer	https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/declaracion.pdf	Sí		1.3.6.1.5.5.7.2.1
2.5 Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.6 cRLDistributionPoint		Sí		OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.6.1 distributionPoint	ldap://ldapsdca2.securitydata.net.ec/CN=AUTORIDAD DE CERTIFICACION RAIZ CA-2 SECURITY DATA,OU=ENTIDAD DE CERTIFICACION DE INFORMACION,O=SECURITY DATA S.A. 2,C=EC?authorityRevocationList?base	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.6.2 distributionPoint		No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7 Authority Information Access		No	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.7.1 Access Method		No		OID 1.3.6.1.5.5.7.48.1
2.7.2 Access Location		No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.7.3 Access Location		No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8 Basic Constraints		Sí	Sí	OID 2.5.29.19
2.8.1 Subject type	Subject is a CA	Sí		
2.8.2 Path Length Constraints	None	Sí		

7.1.1. Número de Versión.

Los certificados siguen el estándar X.509 versión 3 para los suscriptores y versión 2 para las CRLs.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	76

7.1.2. Extensión de los Certificados (OID-Objeto Identificador).

Las extensiones aquí presentadas corresponden con todas las que pueden contener los certificados emitidos. En la Política de Certificación de cada tipo de certificado, se especifican a detalle las extensiones requeridas.

Tabla 2. Extensión de los certificados (OID)

EXTENSIÓN	CRÍTICA	DESCRIPCIÓN
Authority Key Identifier	No	Identificador de la clave del emisor
Subject Key Identifier	No	Identificador de la clave del suscriptor
Key Usage	Sí	Usos permitidos del certificado
Certificate Policies	No	Política de certificación correspondiente al certificado.
Subject Alternative Names	No	Nombre alternativo el suscriptor
Extended Key Usage	No	Define el propósito específico del certificado
cRLDistributionPoint	No	URL oficial donde se publican las CRL
Authority Information Access	No	CA del emisor y OCSP (validación en línea del estado del certificado)
Basic Constraints	Si	Diferencia certificados de usuario y de autoridad.

7.1.3. Identificadores de objetos de algoritmo.

Para la emisión y validación del certificado, la AC emplea los siguientes Identificadores de Objeto (OID) asociados a los algoritmos criptográficos utilizados:

Categoría	Nombre / Descripción	OID	Observación
Algoritmo de clave pública	RSA (PKCS #1) / rsaEncryption	1.2.840.113549.1.1.1	Clave pública RSA 2048 bits
Algoritmo de firma del certificado	sha256WithRSAEncryption	1.2.840.113549.1.1.11	Firma del certificado con SHA-256 + RSA
Algoritmo hash	SHA-256 / id-sha256	2.16.840.1.101.3.4.2.1	Función hash asociada
EKU (Uso extendido)	Autenticación de cliente / id-kp-clientAuth	1.3.6.1.5.5.7.3.2	Presente en el certificado
EKU (Uso extendido)	Protección de correo (S/MIME) / id-kp-emailProtection	1.3.6.1.5.5.7.3.4	Presente en el certificado

Key Usage del certificado (no son OID, son “bits”)

Extensión	Valor en el certificado
-----------	-------------------------

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	77

digitalSignature	TRUE
contentCommitment (no repudio)	TRUE
keyEncipherment	TRUE
dataEncipherment	FALSE
keyAgreement	FALSE
keyCertSign	FALSE
cRLSign	FALSE

7.1.4. Formas de los nombres.

Los certificados emitidos bajo Security Data contienen el "nombre completo", en formato X.500, para el emisor y el suscriptor, situado en los campos "Nombre del emisor" y "Nombre de sujeto", respectivamente, y se forman como se define en la *Tabla 3*.

Tabla 3. Formatos de nombre

CAMPO DEL DN	NOMBRE	DESCRIPCIÓN
CN, Common Name	Nombre del Suscriptor	Nombre y Apellidos del suscriptor
CN, Common Name	Nombre de la CA	Nombres y Apellidos de la CA
OU, Organizational Unit	Unidad Organizacional	Entidad de Certificación de Información
O, Organization	Organización	Nombre de la AC
C, Country	País	Código de país de dos Dígitos según ISO 3166-1. Por defecto "ES".

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.

7.1.6. Identificador de objeto de Política de Certificado.

El identificador de objeto de la Política de certificado correspondiente a cada tipo de certificado, conforme se establece en la Política de Certificación de los certificados de Security Data, cualquier cambio será comunicado a la Autoridad Competente, el formato general es 1.3.6.1.4.1.37746.2.x.x donde los últimos valores corresponden al tipo de certificado. Y Para sello de tiempo y Sellado electrónico el formato general es 1.3.6.1.4.1.37746.102.2.x.x

7.1.7. Uso de la extensión Restricciones de política.

No se estipula.

7.1.8. Sintaxis y semántica de los calificadores de políticas.

El calificador de la política está definido en la extensión de "Certificate Policies" y contiene una referencia al URL donde esta publicada la CPS del proveedor de servicios de certificación.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	78

Tabla 4: Semántica de los Policy Qualifiers

Campo		Obligatorio	Crítico	Observaciones
2.4. Certificate Policies	-	SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information	Información de la Política	SI	-	-
2.4.1.1. Policy Identifier	1.3.6.1.4.1.37746.2.1 .1 – Identificador de la Política	SI	-	Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		SI	-	-
2.4.1.1.1 CPS URI	(https://www.repoexchange.com/dpc/) – URI DPC o PC	SI	-	OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Autoridad de Certificación
2.4.1.1.2. User Notice/Explicit text	Tipo de Certificado	SI	-	OID 1.3.6.1.5.5.7.2.2 Texto indicativo

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

No se estipula.

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 versión 3 de la 5280 " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Las CRL's son firmadas por la autoridad de certificación que ha emitido los certificados.

7.2.1. Número de Versión.

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

7.2.2. CRL y Extensiones de entrada CRL.

CRL de la Autoridad Raíz (AC Root).

Tabla 5: CRL de la autoridad Raíz

CAMPOS	VALORES
Versión	2
Número de CRL	Número incremental
Algoritmo de firma	sha256RSA
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempo UTC)

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	79

Fecha de próxima actualización	Fecha efectiva de emisión + 6 meses
Identificador de la clave de autoridad	Hash de la clave del emisor
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	SI
Lista de revocación de certificados (CRL) indirecta	NO
Entradas de la CRL	Número de serie del certificado Fecha de revocación Código de razón

CRL de las Autoridades de Certificación Subordinadas.

Tabla 6: CRL de las autoridades de certificación subordinadas.

CAMPOS	VALORES
Versión	2
Número de CRL	Número incremental
Algoritmo de firma	sha256RSA
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempoUTC)
fecha de próxima actualización	Fecha efectiva de emisión + 1 días
Identificador de la clave de autoridad	Hash de la clave del emisor
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO
Lista de revocación de certificados (CRL) indirecta	NO
Entradas de la CRL	Número de serie del certificado Fecha de revocación Código de razón

7.3. Perfil OCSP.

7.3.1. Número(s) de versión.

El perfil OCSP corresponde con el propuesto en las Políticas de Certificación correspondientes y con el estándar X.509 versión 3.

7.3.2. Extensiones OCSP.

El perfil OCSP se especifica en la siguiente tabla:

CAMPO	CONTENIDO
1. Basic structure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.
1.3. Signature Algorithm	
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable

CÓDIGO	SD-ID-PE-09
VERSIÓN	V13
FECHA DE APROBACIÓN	26/03/2026
PÁGINAS	80

1.4. Issuer	
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)
1.4.3. Organizational Unit Name (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA
1.4.4. Organization Name(O)	Nombre de la AC Subordinada "Organización"
1.4.5. Common Name (CN)	Nombre de la AC Subordinada
1.5. Validity	Se recomienda (máximo 5 años)
1.5.1. Not Before	Fecha de inicio de validez
1.5.2. Not After	Fecha de expiración
1.6. Subject	
1.6.1. Country Name (C)	Código de País "EC" (ISO 3166)
1.6.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) ej. QUITO
1.6.3. Organization Unit Name (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA
1.6.4. Organization Name (O)	Nombre de la AC Subordinada "Organización"
1.6.5. Common Name (CN)	Nombre de la AC Subordinada
1.6.6. Organization Identifier	"VAT(CÓDIGO_PAIS)-RUC Ej. VATEC-1716151413001
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del Issuer
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del Subject
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado "1"
2.3.2. Content commitment	Seleccionado "1"
2.3.3. Key Encipherment	No seleccionado. "0"
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	
2.4.1. Policy Information	

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	81

2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1
2.4.1.2. Policy Qualifiers	
2.4.1.1.1 CPS URI	(https://www.repo_example.com/dpc/)
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE VALIDACION OCSP"
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Correo electrónico de la Entidad Acreditada "info@example.com.ec"
2.6. Extended Key Usage	
2.6.1. ocspSigning	Presente (1.3.6.1.5.5.7.3.9)
2.6.2. ocspNoCheck	Presente (1.3.6.1.5.5.7.48.1.5)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	(http://crl1.example.com/example1subordinada.crl)
2.7.2. distributionPoint	(http://crl2.example.com/example2subordinada.crl)
2.8. Authority Information Access	
2.8.1. Access Description	
2.8.1.1. Access Method	id-ad-calssuers
2.8.1.1.1 Access Location	(http://ocsp1.example.com/subordinate1.crt)
2.9. Basic Constraints	
2.9.1. cA	FALSE

8. AUDITORÍAS DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

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

8.1. Frecuencia o circunstancias de la evaluación.

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

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

8.2. Cualificación del auditor.

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

8.3. Relación entre el auditor y la entidad 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 Seguridad en Datos y Firma Digital.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	82

No obstante, Security Data Seguridad en Datos y Firma Digital 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. Temas cubiertos por la evaluación.

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 (la presente 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.

Auditoría en las Autoridades de Registro.

Las Autoridades de Registro que tengan acceso al software/sistema facilitado por Security Data Seguridad en Datos y Firma Digital para la gestión de certificados, son auditadas por un tercero previamente a su puesta en marcha efectiva. Adicionalmente, se realizan auditorías que comprueban el cumplimiento de los requerimientos exigidos por las Políticas de Certificación para el desarrollo de las labores de registro expuestas en el contrato de servicio firmado. La periodicidad de las auditorías vendrá determinada por el acuerdo entre Security Data Seguridad en Datos y Firma Digital y la Autoridad de Registro, siempre teniendo en cuenta la actividad prevista a desarrollar por la Autoridad de Registro en cuanto a número de certificados o requerimientos específicos de seguridad.

No obstante, y excepcionalmente, Security Data Seguridad en Datos y Firma Digital podría eximir a una Autoridad de Registro de la obligación de someterse a una auditoría inicial y a las auditorías de mantenimiento.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	83

8.5. Acciones adoptadas como resultado de la deficiencia.

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

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

8.6. Comunicación de resultados.

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

Security Data publicará los informes vigentes y sello Webtrust en su página web <https://www.securitydata.net.ec/nosotros-security-data-ecuador/>

Security Data anualmente ejecutará la auditoria a la normativa técnica según los plazos establecidos por la entidad reguladora, cuyo informe será puesto a disposición de ARCOTEL 15 días después de finalizado el proceso.

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD.

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 área de operaciones de Security Data Seguridad en Datos y Firma Digital o por medio de la página web: www.securitydata.net.ec.

El detalle de los precios por Emisión de una firma electrónica sea esta de persona natural o jurídica son los siguientes:

- Vigencia de una semana \$5,15 incluye IVA
- Vigencia de un mes \$12,10 incluye IVA
- Vigencia de 1 año \$24,15 incluye IVA
- Vigencia de 2 años \$36,57 incluye IVA
- Vigencia de 3 años \$51,22 incluye IVA
- Vigencia de 4 años \$63,64 incluye IVA
- Vigencia de 5 años \$74,41 incluye IVA

Para la renovación de firmas electrónicas se aplicará el siguiente descuento sobre el valor de emisión de firmas electrónicas:

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	84

- Todas las renovaciones de firmas con vigencia de un año, tendrán un descuento del 10%.

Se tendrá como regla para aplicar descuentos para las renovaciones de firmas de vigencia de más de un año, que, se debe solicitar la renovación con la firma aún vigente o hasta 30 días después de su caducidad, y cumplir las siguientes condiciones:

- Si el suscriptor realiza su primera renovación de firma o es el segundo producto de firma que adquiere (Ejemplo: Tenía una firma como persona natural y ahora desea una firma como persona jurídica) y cumple la Regla tiene un descuento del 15%.
- Si un suscriptor realiza su segunda renovación de firma o es el tercer producto de firma que adquiere (Ejemplo: 2 firmas como persona natural y ahora desea una firma como persona jurídica) y cumple la Regla tiene un descuento del 20% (Solo en la vigencia de dos años), para vigencias de 3 años, 4 años y 5 años la renovación tiene un descuento del 15%.

En caso de requerir un dispositivo DSCF para resguardar la firma electrónica, se cobrará un valor de \$13,80 incluido el IVA por el dispositivo.

Nota: En caso de que el suscriptor requiera hacer un cambio de contraseña de su certificado, se emitirá un certificado nuevo, este servicio tendrá un valor de \$5,75 incluido IVA.

Los pagos se realizarán previo a la emisión del certificado, estos se podrán realizar con tarjeta de crédito o débito cuando la solicitud sea realizada de forma presencial, si es en línea se podrá realizar este tipo de pagos mediante un link seguro de pago o depósito o transferencia bancaria adjuntando el comprobante o llevándolo a las oficinas de Security Data.

9.1.2. Tarifas de Acceso a los Certificados.

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 Estado o Revocación.

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.

9.1.4. Tarifas 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.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	85

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

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

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

En 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 Autoridad de Certificación de Security Data en el desarrollo de las actividades para las cuales cuenta con autorización.

9.2.2. Otros activos.

Sin estipulación.

9.2.3. Cobertura de seguro o garantía para entidades finales.

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

9.3. Confidencialidad de la información 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.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	86

9.3.1. Alcance de la Información Confidencial.

Security Data Seguridad en Datos y Firma Digital considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difundirá información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

- Las claves privadas de firma de los suscriptores son confidenciales y no se proporcionan a la AC ni a los terceros vinculados.
- La información específica para la operación y el control de la AC, como los parámetros de seguridad y las pistas de auditoría, es mantenida de manera confidencial por la AC y no se divulga fuera de la organización de la AC a menos que la ley lo exija.
- La información sobre los suscriptores en poder de la AC o terceros vinculados, excluyendo la que se publica en los certificados, las CRL, las Políticas de Certificados o esta DPC, se considera confidencial y no se divulgará fuera de la AC a menos que lo exija la Política de Certificación o la ley.
- Otras circunstancias de divulgación de información.
- Publicación de información concerniente a la revocación.
- Cualquier otra información relacionada con el suscriptor o SECURITY DATA, que puede ser de naturaleza confidencial.

9.3.2. Información no Confidencial.

La siguiente información será considerada no confidencial:

- La contenida en la presente DPC.
- La contenida en las distintas Políticas de Certificación (PC).
- La información contenida en los certificados, puesto que para su emisión el suscriptor otorga previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de revocación de certificados (CRL's), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Toda la información clasificada expresamente como "PÚBLICA".
- Cualquier información cuya publicidad sea impuesta normativamente.

9.3.3. Responsabilidad en la Protección de Información Confidencial.

Es responsabilidad de Security Data Seguridad en Datos y Firma Digital establecer medidas adecuadas para la protección de la información confidencial.

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

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	87

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

9.4. Privacidad de la información personal.

9.4.1. Política de Privacidad.

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

Security Data trata los datos personales conforme a la Ley Orgánica de Protección de Datos Personales (LOPD), el titular podrá hacer uso de todos sus derechos sobre la información que este proporciona para la emisión de certificados, estos derechos son: Acceso, rectificación, cancelación y oposición.

El titular puede hacer uso de sus derechos mediante el siguiente formulario: https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/Formulario_Derechos_Titulares_Dato_Personal.pdf

El tratamiento se basa en el consentimiento explícito del titular y en el cumplimiento de las obligaciones legales derivadas de la prestación de servicios de certificación.

Los datos se conservarán hasta el cese de funciones como entidad de certificación.

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, es considerada privada.

9.4.3. Información no considerada Privada.

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

9.4.4. Responsabilidad de proteger la información privada.

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

9.4.5. Aviso y Consentimiento para el uso de información privada.

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

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	88

9.4.6. Divulgación en virtud de un proceso judicial o administrativo.

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 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 Declaración de Prácticas de Certificación, PC y a los estándares de aplicación. Además de:

- Emitir Certificados conforme a esta DPC y a lo establecido en la PC y a los estándares de aplicación.
- Emitir Certificados cuyo contenido mínimo sea definido en la DPC y PC 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.
- Facilitar el acceso a las versiones vigentes de la DPC y de las PCs de cada tipo de Certificados.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	89

- Ofrecer y mantener la infraestructura necesaria para los servicios de certificación, así como los controles de seguridad física, de procedimientos y personales necesarios para la práctica de la actividad de certificación.
- Asimismo, emite los certificados 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 Norma Técnica Ecuatoriana y 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.
- 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.
- Informar sobre las modificaciones de las Políticas de Certificados y de la Declaración de Prácticas de Certificación a los Suscriptores y Terceros vinculados.
- Cumplir con las obligaciones del presente DPC.
- Todas aquellas obligaciones impuestas por el presente DPC y en su caso, en la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos y Norma Técnica Ecuatoriana.
- Aprobar o negar las solicitudes de emisión de certificados digitales de firma electrónica, de acuerdo con lo establecido en esta DPC y en las PCs.
- Poner a disposición de los usuarios el listado de certificados revocados (CRL).
- Custodiar por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante toda la vigencia de la acreditación, de manera que puedan verificarse las firmas efectuadas con el mismo. A estos efectos, SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL almacena en formato digital o en papel todas las versiones de la DPC publicadas y copia del contrato de prestación de servicios entre la Entidad de Certificación de Información y el suscriptor.
- Comunicar de manera inmediata a los titulares de los certificados emitidos por la ECI, el compromiso de su clave privada, pérdida, divulgación, modificación, uso no autorizado, con el fin de revocarlos.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	90

- Efectuar la identificación y autenticación de los usuarios como pasos previos a la revocatoria de los certificados de firma electrónica.
- Proteger los datos personales de los solicitantes y usuarios de certificados digitales o electrónicos.
- Llevar a cabo cada uno de los pasos que se describan en el procedimiento de emisión de certificados de firma electrónica.
- Implementar y mantener los requerimientos de seguridad impuestos a la clave privada de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, de acuerdo a esta DPC y PCs.
- Ofrecer y mantener la infraestructura tecnológica necesaria para el establecimiento de una estructura, tanto en hardware como en software, para operar de acuerdo a los estándares internacionales.
- Conservar toda la información y documentación relativa a cada Certificado, en las debidas condiciones de seguridad, durante toda la vigencia de la acreditación contados desde el momento de la expedición del certificado raíz, de manera que puedan verificarse las firmas efectuadas con el mismo.
- Presentar la lista actualizada de los terceros vinculados que forman parte de la entidad de certificación Security Data aprobados por ARCOTEL, las cuales se puede consultar en el siguiente enlace: https://www.securitydata.net.ec/wp-content/downloads/terceros_vinculados.pdf

9.6.2. Declaraciones y Garantías de la RA.

Las responsabilidades de la entidad de registro son las siguientes:

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

El Tercero Vinculado podrá asumir las siguientes obligaciones de las cuales será responsable:

- Identificar y autenticar correctamente al Suscriptor y/o Solicitante y/o a la organización que represente, conforme a los procedimientos que se establecen en esta DPC y en las Prácticas de Certificación específicas para cada tipo de Certificado, utilizando cualquiera de los medios admitidos en derecho.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	91

- Formalizar los contratos de expedición de los certificados con el Suscriptor en los términos y condiciones que establezca la AC.
- Almacenar de forma segura y por un periodo nunca inferior a 15 años la documentación aportada en el proceso de emisión del Certificado y en proceso de suspensión / revocación del mismo, en los términos y condiciones que se establezcan en esta DPC, en la PC de cada tipo de certificado y, en su caso, en el acuerdo para el Tercero Vinculado.
- Llevar a cabo cualquier otra función que les correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta DPC y en la PC de cada tipo de certificado y, en su caso, el Acuerdo para el Tercero Vinculado.
- En todo caso el Tercero Vinculado permitirá a SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL el acceso a los archivos y a los procedimientos de conservación de los archivos asumidos por el Tercero Vinculado y le dará el derecho a investigar cualquier sospecha de infracción de la DPC y/o de las PC por parte del Tercero Vinculado o cualquier poseedor de un Certificado. El Tercero Vinculado y los poseedores de cualquier Certificado deberán informar a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL inmediatamente de cualquier sospecha de infracción.

9.6.3. Declaraciones y Garantías de los Solicitantes.

- Abonar las tarifas de registro que correspondan en virtud de los servicios que soliciten.
- Suministrar al Tercero Vinculado o a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL la información necesaria para realizar una correcta identificación.
- Confirmar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- Solicitar el certificado según se estipula en los términos y condiciones que se establezcan en la PC de cada tipo de Certificados y, en su caso, en el Contrato para la prestación de servicios de certificados suscrito con la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

9.6.4. 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 la correspondiente Política de Certificado.
- Comunicar a Security Data cualquier modificación o variación de los datos que se aportaron para obtener el Certificado de Firma Electrónica.
- Verificar, a través de la Lista de Certificados Revocados, el estado de los Certificados de firma electrónico.
- Proteger y conservar el Dispositivo Seguro de Creación de Firma.\o a su vez el acceso al certificado en software.
- Solicitar 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 Firma Electrónica.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	92

- Responder por el uso del Certificado de Firma Electrónica 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 DPC.

9.6.5. 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 Autoridad 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.

9.6.6. Declaraciones y Garantías de los Usuarios.

- Los usuarios que pretendan confiar y usar los Certificados emitidos por la AC deberán verificar la validez de las firmas emitidas por los Suscriptores.
- En el supuesto de que los Usuarios no procederían a verificar las firmas a través de la CRL (Lista de Certificados Revocados), la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL no se hace responsable del uso y confianza que los usuarios hagan de estos Certificados.
- Toda persona tendrá derecho a confiar en una firma electrónica emitida mediante un certificado de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL en la medida en que sea razonable hacerlo.
- Para determinar si es razonable confiar; deberá tenerse en cuenta, en su caso, lo siguiente:
 - La Naturaleza de la operación correspondiente que la firma tenga por objeto avalar. No se considerará razonable confiar en una firma emitida por un certificado de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL si dicha operación puede ser considerada un uso indebido.
 - Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad de la firma, y en particular, si ha verificado que el certificado no esté caducado, suspendido o revocado. La caducidad constará en el propio Certificado. La posible suspensión o revocación del certificado deberán ser consultadas en la lista de revocaciones o suspensiones de certificados (CRL).
 - Si la parte que confía sabía o debía haber sabido que la firma estaba entredicha o había sido revocada o suspendida.
- Las políticas y procedimientos que rigen la actividad de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL en relación con las diferentes Firmas Electrónicas realizadas

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	93

con los tipos de certificados emitidos por la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, políticas y procedimientos que se especifican en este DPC y en la PCs para cada tipo de certificado distinto.

Responsabilidades.

a) Responsabilidad de la AC

- Garantizar el cumplimiento de las responsabilidades y obligaciones descritas en esta DPC; y lo previsto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, y su Reglamento.
- La ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, única y exclusivamente, responderá por daños y perjuicios que causen a cualquier persona, cuando incumpla sus obligaciones legales derivadas de la legislación vigente en la República del Ecuador o cuando actúe con la negligencia en la prestación de servicios de certificación.
- La ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL no será responsable de los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del Solicitante, Suscriptor y/o Usuario.
- La ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL no será responsable de la utilización negligente o dolosa de los certificados y las claves.
- La ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL no será responsable de los daños y perjuicios que se deriven de actuaciones negligentes o dolosas por parte de terceros con relación a los certificados por ella emitidos a favor de un determinado suscriptor.
- La ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL no será responsable de las eventuales inexactitudes en el Certificado que resulten de la información facilitada por el Suscriptor, a condición de haber actuado siempre con la máxima negligencia exigible.
- La ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL no será responsable de los daños que se deriven de aquellas operaciones en que se hayan incumplido las limitaciones de uso que se señalan en las PCs correspondientes a cada tipo de certificado.
- La ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud de la presente DPC si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL no pueda tener un control razonable.
- La ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL no será responsable del contenido de aquellos documentos electrónicos firmados digitalmente. Ni la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL ni sus autoridades de registro serán responsables en ningún caso por los daños causados por el empleo de sus servicios de certificación pública en estos entornos.
- La ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL cuenta con la debida póliza de garantía, la cual se renueva cada año y es entregada al ente regulador de acuerdo a la normativa y exigencias de ARCOTEL.
- Las condiciones generales de la póliza se pueden consultar en el siguiente enlace <http://www.securitydata.net.ec/ayuda-security-data->

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	94

ecuador/ en la sección de normativas, ítem 17. “Garantía” donde se hallará la información actualizada de la póliza.

b) Responsabilidad del Tercero vinculado.

- El Tercero Vinculado responderá de las funciones que le correspondan conforme a esta DPC y, en especial, asumirá toda la responsabilidad por la correcta identificación y validación del Solicitante/Suscriptor, con las mismas limitaciones que se establecen en el apartado anterior con relación a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.
- El Tercero Vinculado, responderá ante la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL por los daños y perjuicios que pudieran derivarse de la ejecución de esas funciones concertadas de manera negligente o en forma distinta a la contemplada en la presente DPC y en las PCs emitidas para cada tipo de certificado.
- No obstante, el Tercero Vinculado no se hace responsable, en ningún caso, de la identidad o identificación del solicitante y/o suscriptor en el supuesto de falsificación de la documentación u otros datos aportados, por él mismo o por el tercero que le suplante.

c) Responsabilidad del Suscriptor.

- El Suscriptor será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta DPC.
- El Suscriptor será responsable del cumplimiento de todas aquellas obligaciones impuestas por la presente DPC, las PC de cada tipo de Certificado, y por la normativa vigente en materia de prestación de servicios de certificación.
- El Suscriptor se compromete a indemnizar a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL los daños o perjuicios que puedan ocasionar cualquier acto u omisión culposa o dolosa de su parte, asumiendo igualmente los costos procesales en que la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL pudiera incurrir por esta causa, incluyendo los honorarios profesionales de Abogados y Procuradores.
- El Suscriptor indemnizará y mantendrá indemne a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL por cualquier daño que esta pudiera sufrir por el cumplimiento total, parcial o defectuoso de las obligaciones asumidas y en base a toda reclamación dirigida contra ella por cualquier tercero con lo que el suscriptor hubiera contratado.

d) Responsabilidad del Usuario.

- El Usuario será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta DPC.
- El Usuario será responsable del cumplimiento de todas aquellas obligaciones impuesta por la presente DPC, las PC de cada tipo de Certificado, y por la normativa vigente en materia de prestación de servicios de certificación.
- En todo caso, el Usuario asumirá toda la responsabilidad y riesgos derivados de la aceptación de un Certificado sin haber observado las obligaciones recogidas en la DPC y, en su caso, en las PC específicas de cada certificado, garantizando la plena indemnidad de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL por dicho concepto.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	95

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 DPC y su correspondiente PC.

9.8. Limitaciones de responsabilidad.

En la medida en que la CA de SECURITY DATA, haya emitido y administrado el certificado de firma electrónica de acuerdo con la DPC y su correspondiente PC, 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 DPC y su correspondiente PC, 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 lo establecido en la presente DPC y su PC.

La responsabilidad de SECURITY DATA, a cualquier persona por daños que surjan bajo, fuera o relacionado con esta DPC y su PC, 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 Declaración de Prácticas de Certificación y cualquier enmienda a este, entrarán en vigencia tras su publicación en la web de SECURITY DATA y permanecerán vigentes hasta que sea reemplazado por una versión más nueva.

9.10.2. Terminación.

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

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	96

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. Pudiendo también notificar de manera directa y expedita a los titulares afectados y a la Autoridad de Protección de Datos, conforme a los plazos legales establecidos.

9.12. Enmiendas.

Las enmiendas y cambios serán comunicadas a 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. Las diferencias que se presenten entre las partes con ocasión de este Servicio durante su ejecución o por su interpretación serán resueltas en primera instancia directamente entre el Usuario y SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.

De no existir dicho acuerdo, podrán someter la controversia al proceso de mediación como un sistema alternativo de solución de conflictos reconocido constitucionalmente, para lo cual las partes estipulan acudir al Centro de Mediación de la Procuraduría General del Estado.

El proceso de mediación se sujetará a la Ley de Arbitraje y Mediación y al Reglamento de Funcionamiento del Centro de Mediación de la Procuraduría General del Estado.

Si se llegare a firmar una Acta de acuerdo total, la misma tendrá efecto de sentencia ejecutoriada y cosa juzgada y su ejecución será del mismo modo que las sentencias de última instancia siguiendo la vía de apremio, conforme lo dispone el Art. 47 de la Ley de Arbitraje y Mediación.

En el caso de no existir acuerdo de las partes, suscribirán la respectiva acta de imposibilidad de acuerdo, y la controversia se ventilará ante el Tribunal Distrital de lo Contencioso Administrativo competente.

En el caso de suscribirse actas de acuerdo parcial, las mismas tendrán efecto de cosa juzgada sobre los asuntos acordados; y para el caso de aspectos sobre los cuales no se acuerde, éstos serán resueltos ante el Tribunal Distrital de lo Contencioso Administrativo competente.

9.14. Ley aplicable.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento; Ley Orgánica de Protección de Datos Personales (LOPDP) 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

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	97

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.

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 Declaración de Prácticas de Certificación, 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 Declaración de Prácticas de Certificación y en su PC, se considera inválida por una autoridad competente en la jurisdicción aplicable, el resto de la Declaración de Prácticas y Política de Certificación seguirá siendo válido y exigible.

9.16.4. Ejecución.

Sin estipulación.

9.16.5. Fuerza Mayor.

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

9.17. Otras disposiciones.

Sin estipulación.

10. CONTROL DE APROBACIONES.

 <p>SECURITYDATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.</p>	<p align="center">DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN</p>	CÓDIGO	SD-ID-PE-09
		VERSIÓN	V13
		FECHA DE APROBACIÓN	26/03/2026
		PÁGINAS	98

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