

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	1



DECLARACIÓN DE
POLÍTICAS DE SEGURIDAD

febrero 18

2026

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	2

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	FECHA	ELABORADO POR	REVISADO POR	APROBADO POR
V1	Edición Inicial	11/02/2011	Gerente Técnico	Gerente Técnico	Gerente General
V2	Actualización general de la DPS conforme a la Normativa Técnica.	18/02/2026	Coordinador del Sistema de Gestión	Chief Technology Officer (CTO) Supervisor Legal	Gerente General

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	3

Contenido

1.	Marco Legal.....	9
1.1.	BASE LEGAL.....	9
1.2.	VIGENCIA.....	9
1.3.	SOPORTE LEGAL.....	9
2.	Introducción.....	10
2.1.	PRESENTACIÓN.....	10
2.2.	NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN DEL DOCUMENTO.....	10
2.3.	ENTIDADES PARTICIPANTES.....	10
2.3.1.	Entidad Acreditada (EA).....	10
2.3.2.	Autoridad de Certificación (AC).....	10
2.3.3.	Autoridad de Certificación Raíz.....	11
2.3.4.	Autoridad de Registro (AR).....	11
2.3.5.	Solicitante.....	12
2.3.6.	Suscriptor.....	12
2.3.7.	Firmante.....	12
2.3.8.	Custodio de las Claves.....	12
2.3.9.	Tercero que Confía en los Certificados.....	12
2.4.	USO DEL CERTIFICADO.....	13
2.4.1.	Usos Apropiados de los Certificados.....	13
2.4.2.	Usos Prohibidos de los Certificados.....	13
2.5.	ADMINISTRACIÓN DE POLITICAS.....	13
2.5.1.	Organización que administra el Documento.....	13
2.5.2.	Persona de Contacto.....	13
2.5.3.	Persona que determina la idoneidad del CPS para la Política.....	13
2.5.4.	Procedimientos de aprobación de la DPS.....	14
2.6.	DEFINICIONES Y ACRÓNIMOS.....	14
2.6.1.	Definiciones.....	14
2.6.2.	Acrónimos.....	15
3.	Responsabilidades de Publicación y Repositorio.....	16
3.1.	REPOSITORIOS.....	16
3.2.	PROCEDIMIENTO DE APROBACIÓN.....	16
3.3.	TIEMPO O FRECUENCIA DE PUBLICACIÓN.....	16

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	4

3.4.	CONTROLES DE ACCESO A LOS REPOSITORIOS	17
4.	Identificación y Autenticación.....	17
4.1.	DENOMINACIÓN.	17
4.1.1.	Tipos de Nombres.	17
4.1.2.	Necesidad de que los nombres sean significativos.....	17
4.1.3.	Reglas para interpretar varios formatos de nombres.....	17
4.1.4.	Unicidad de los nombres.....	17
4.1.5.	Reconocimiento, autenticación y función de las marcas.....	17
4.2.	VALIDACIÓN INICIAL DE LA IDENTIDAD.....	17
4.3.	IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN DE CLAVES. 17	
4.4.	IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA SOLICITUD DE REVOCACIÓN.....	17
5.	Requisitos Operacionales del Ciclo de Vida del Certificado.....	18
5.1.	SOLICITUD DEL CERTIFICADO.....	18
5.2.	TRAMITACIÓN DE LA SOLICITUD DEL CERTIFICADO.....	18
5.3.	EMISIÓN DEL CERTIFICADO.....	18
5.4.	ACEPTACIÓN DEL CERTIFICADO.....	18
5.5.	USO DE PARES DE CLAVES Y CERTIFICADOS.....	18
5.6.	RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVE.....	18
5.7.	RENOVACIÓN CON CAMBIO DE CLAVE DEL CERTIFICADO.....	18
5.8.	MODIFICACIÓN DEL CERTIFICADO.....	18
5.9.	REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO.....	18
5.10.	SERVICIO DE ESTADO DE CERTIFICADO.....	18
5.10.1.	Características Operativas.....	18
5.10.2.	Disponibilidad del Servicio.....	19
5.10.3.	Características Opcionales.....	19
5.11.	FIN DE LA SUSCRIPCIÓN.....	19
5.12.	CUSTODIA Y RECUPERACIÓN DE CLAVES.....	19
5.12.1.	Política y prácticas de depósito y recuperación de claves.....	19
5.12.2.	Política y prácticas de encapsulación y recuperación de claves de sesión.....	19
6.	Controles de Instalaciones, Gestión y Operación.....	19
6.1.	CONTROLES FÍSICOS.....	19
6.1.1.	Ubicación física y construcción.....	20

CÓDIGO	SD-ID-PE-15
VERSIÓN	V2
FECHA DE APROBACIÓN	18/02/2026
PÁGINAS	5

6.1.2.	Acceso Físico.....	20
6.1.3.	Alimentación Eléctrica y Aire Acondicionado.	20
6.1.4.	Exposición al Agua.....	21
6.1.5.	Protección y Prevención de Incendios.	21
6.1.6.	Sistema de Almacenamiento.....	21
6.1.7.	Eliminación de los Soportes de Información.....	21
6.1.8.	Seguridad de la Información Empresarial.	21
6.2.	CONTROLES DE PROCEDIMIENTO.	21
6.2.1.	Roles de Confianza.	21
6.2.2.	Número de personas necesarias por tarea.	22
6.2.3.	Identificación y autenticación por cada rol.....	22
6.2.4.	Roles que requieren separación de funciones.	23
6.3.	CONTROLES DE PERSONAL.....	23
6.3.1.	Requisitos sobre la Cualificación, Experiencia y Conocimientos Profesionales..	23
6.3.2.	Procedimiento de Comprobación de Antecedentes.....	23
6.3.3.	Requerimientos de Formación.....	23
6.3.4.	Requisitos y Frecuencia de Actualización de Formación.	24
6.3.5.	Frecuencia y Secuencia de Rotación de Tareas.....	24
6.3.6.	Sanciones por Actuaciones No Autorizadas.....	24
6.3.7.	Requisitos de Contratación de Personal.	24
6.3.8.	Documentación Proporcionada al Personal.....	24
6.4.	PROCEDIMIENTOS DE REGISTRO DE AUDITORÍA.	25
6.4.1.	Tipos de Eventos Registrados.....	25
6.4.2.	Frecuencia de Procesado de Registros de Auditoría.....	25
6.4.3.	Periodo de Conservación de los Registros de Auditoría.	26
6.4.4.	Protección de los Registros.	26
6.4.5.	Procedimientos de Respaldo de los Registros de Auditoría.....	26
6.4.6.	Sistema de Recolección de Información de Auditoría.	26
6.4.7.	Notificación de Eventos.....	26
6.4.8.	Análisis de Vulnerabilidades.....	27
6.5.	ARCHIVO DE REGISTRO.	27
6.5.1.	Tipo de Eventos Archivados.	27
6.5.2.	Periodo de Conservación de Registros.....	27
6.5.3.	Protección del Archivo.	27

CÓDIGO	SD-ID-PE-15
VERSIÓN	V2
FECHA DE APROBACIÓN	18/02/2026
PÁGINAS	6

6.5.4.	Procedimientos de Copia de Seguridad del Archivo.	28
6.5.5.	Requerimientos para el Sellado de Tiempo de los Registros.	28
6.5.6.	Sistema de Archivo de Información de Auditoría.	28
6.5.7.	Procedimientos para obtener y verificar información de archivo.	28
6.6.	CAMBIO DE CLAVE DE LA AC.	28
6.6.1.	AC Raíz.	28
6.6.2.	AC Subordinada.	29
6.7.	COMPROMISO Y RECUPERACIÓN ANTE DESASTRES.	29
6.7.1.	Procedimientos de Gestión de Incidentes y Vulnerabilidades.	29
6.7.2.	Alteración de los Recursos Hardware, Software y/o Datos.	29
6.7.3.	Procedimiento de Actuación ante la Vulnerabilidad de la Clave Privada de la AC. 29	
6.7.4.	Continuidad del Negocio después de un desastre.	30
6.8.	TERMINACIÓN DE CA O RA.	30
6.8.1.	Autoridad de Certificación.	30
6.8.2.	Autoridad de Registro.	30
7.	Controles Técnicos de Seguridad.	31
7.1.	GENERACIÓN E INSTALACIÓN DE PARES DE CLAVES.	31
7.2.	PROTECCIÓN DE CLAVES PRIVADAS E INGENIERÍA DE MÓDULOS CRIPTOGRÁFICOS.	31
7.2.1.	Estándares para los Módulos Criptográficos.	31
7.2.2.	Control Multipersona (k de n) de la Clave Privada.	31
7.2.3.	Custodia de la Clave Privada.	31
7.2.4.	Copia de Seguridad de la Clave Privada de la AC.	31
7.2.5.	Archivo de la Clave Privada del Suscriptor.	32
7.2.6.	Transferencia de la Clave Privada a/o desde el Módulo Criptográfico.	32
7.2.7.	Almacenamiento de clave privada en el módulo criptográfico.	32
7.2.8.	Método de Activación de la Clave Privada.	33
7.2.9.	Método de Desactivación de la Clave Privada.	33
7.2.10.	Método de Destrucción de la Clave Privada.	33
7.2.11.	Clasificación del módulo criptográfico.	34
7.3.	OTROS ASPECTOS DE LA GESTIÓN DE PARES DE CLAVES.	34
7.3.1.	Archivo de la Clave Pública.	34
7.3.2.	Periodos operativos de los Certificados y Periodo de uso del Par de Claves.	34
7.4.	DATOS DE ACTIVACIÓN.	34

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	7

7.4.1.	Generación e Instalación de los Datos de Activación.	34
7.4.2.	Protección de los Datos de Activación.	34
7.4.3.	Otros aspectos de los datos de activación.	34
7.5.	CONTROLES DE SEGURIDAD INFORMÁTICA.....	35
7.5.1.	Requerimientos Técnicos de Seguridad Específicos.	35
7.5.2.	Clasificación de la Seguridad Informática.	35
7.6.	CONTROLES TÉCNICOS DEL CICLO DE VIDA.	36
7.6.1.	Controles de Desarrollo de Sistemas.	36
7.6.2.	Controles de Gestión de Seguridad.....	36
7.6.3.	Controles de Seguridad del Ciclo de Vida.	37
7.7.	CONTROLES DE SEGURIDAD DE LA RED.	37
7.8.	SELLADO DE TIEMPO.	38
8.	Perfiles de Certificados, CRL y OCSP.	38
8.1.	PERFIL DEL CERTIFICADO.....	38
8.2.	PERFIL CRL.	38
8.3.	PERFIL OCSP.	38
9.	Auditoría de Cumplimiento y Otras Evaluaciones.....	38
9.1.	FRECUENCIA DE LAS AUDITORIAS.	38
9.2.	CUALIFICACIÓN DEL AUDITOR.	38
9.3.	RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA.....	38
9.4.	ASPECTOS CUBIERTOS POR LOS CONTROLES.....	38
9.5.	ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE INCIDENCIAS. .	39
9.6.	COMUNICACIÓN DE RESULTADOS.	39
10.	Otros asuntos comerciales y legales.	39
10.1.	TARIFAS.	39
10.2.	RESPONSABILIDAD FINANCIERA.....	39
10.3.	CONFIDENCIALIDAD DE LA INFORMACIÓN EMPRESARIAL.	39
10.3.1.	Alcance de la Información Confidencial.	39
10.3.2.	Información No Confidencial.....	40
10.3.3.	Deber de Proteger la Información Confidencial.....	40
10.4.	PRIVACIDAD DE LA INFORMACIÓN PERSONAL.	40
10.4.1.	Política de Privacidad.	40
10.4.2.	Información tratada como Privada.	40

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	8

10.4.3.	Información No Calificada como Privada.	40
10.4.4.	Responsabilidad de la Protección de los Datos de Carácter Personal.	41
10.4.5.	Notificación y Consentimiento para usar Datos de Carácter Personal.	41
10.4.6.	Revelación en el marco de un proceso administrativo o judicial.....	41
10.4.7.	Otras circunstancias de revelación de información.	41
10.5.	DERECHOS DE PROPIEDAD INTELECTUAL.	41
10.6.	DECLARACIONES Y GARANTÍAS.	41
10.7.	RENUNCIAS A GARANTÍAS.....	41
10.8.	LIMITACIONES DE RESPONSABILIDAD.....	41
10.9.	INDEMNIZACIONES.	42
10.10.	PLAZO Y TERMINACIÓN.....	42
10.10.1.	Plazo.	42
10.10.2.	Terminación.....	42
10.11.	AVISOS Y COMUNICACIONES INDIVIDUALES.	42
10.12.	ENMIENDAS.....	42
10.13.	RESOLUCIÓN DE DISPUTAS.	42
10.14.	LEY APLICABLE.....	42
10.15.	CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE.....	42
10.16.	DISPOSICIONES DIVERSAS.	43
10.17.	OTRAS DISPOSICIONES.....	43
11.	Control de Aprobaciones.....	43

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	9

1. Marco Legal.

1.1. BASE LEGAL.

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

1.2. VIGENCIA.

El presente documento entrará en vigencia a partir de la fecha de su aprobación.

1.3. SOPORTE LEGAL.

- a) Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial No. 577 de 17 de abril de 2002.
- b) De conformidad con lo dispuesto en el Art. 37 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el Consejo Nacional de Telecomunicaciones es el Organismo de autorización, registro y regulación de las Entidades de Certificación de Información y Servicios Relacionados Acreditados.
- c) Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedido mediante Decreto Ejecutivo No. 3496 publicado en el Registro Oficial 735 de 31 de diciembre de 2002, y reformas constantes en Decreto Ejecutivo 1356 de 29 de septiembre de 2008, publicadas en el Registro Oficial No. 440 de 6 de octubre de 2008.
- d) Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459, 26 de mayo de 2021, la cual rige el tratamiento, almacenamiento y protección de la información de los titulares de certificados.
- e) Que, el segundo artículo enumerado agregado por el artículo 4 del Decreto Ejecutivo No. 1356 a continuación del artículo 17 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, dispone que la acreditación como entidad de certificación de información y servicios relacionados, consistirá en un acto administrativo emitido por el CONATEL a través de una resolución que será inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados.
- f) Resolución 477-20-CONATEL-2008 de 08 de octubre de 2008, se aprobó el modelo de resolución para la Acreditación como Entidad de Certificación de Información y Servicios Relacionados.
- g) Resolución No. TEL-640-21-CONATEL-2010 de 22 de octubre de 2010, aprobó la petición de Acreditación de la Compañía SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. como Entidad de Certificación de Información y Servicios Relacionados, para los cual la SENATEL suscribió el respectivo acto administrativo, conforme el modelo aprobado por el Consejo Nacional de Telecomunicaciones.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	10

2. Introducción.

2.1. PRESENTACIÓN.

El presente documento contempla la Declaración de Políticas de Seguridad (DPS) de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A., en adelante Security Data.

Esta DPS contempla lo establecido en la DPC de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL estableciendo un conjunto de reglas que indican los procedimientos seguidos por la Entidad de Certificación en cuanto a la seguridad en su infraestructura.

Esta Declaración de Políticas de Seguridad (DPS), junto con la DPC de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, están dirigidas a cualquiera que confíe en esta AC.

2.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN DEL DOCUMENTO.

Nombre:	Declaración de Políticas de Seguridad (DPS)
Código:	SD-ID-PE-15
Versión:	2
Descripción:	Declaración de Políticas de Seguridad de Security Data Seguridad en Datos y Firma Digital S.A.
Fecha de Publicación:	18 de febrero del 2026
Tipo de documento:	Público

2.3. ENTIDADES PARTICIPANTES.

2.3.1. 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, sellado de tiempo y sello electrónico, regidos por sus políticas particulares, no incluidas en este documento.

2.3.2. 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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	11

2.3.3. Autoridad de Certificación Raíz.

Se denomina Autoridad de Certificación Raíz (AC 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.

2.3.4. Autoridad de Registro (AR).

Una Autoridad de Registro (en inglés RA o Registration Authority) 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 del certificado al suscriptor.

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

- Cualquier persona jurídica que sea cliente de Security Data Seguridad en Datos y Firma Digital, para la emisión de certificados a nombre de la corporación o a miembros de la corporación, y que cumpla con los requisitos técnicos y de seguridad exigidos por la entidad y el órgano de control, para la emisión de certificados.
- Cualquier entidad de confianza que llegue a un acuerdo con Security Data Seguridad en Datos y Firma Digital para actuar como intermediario en nombre de Security Data Seguridad en Datos y Firma Digital.
- La propia Security Data Seguridad en Datos y Firma Digital directamente.

Security Data Seguridad en Datos y Firma Digital formalizará contractualmente las relaciones entre ella y cada una de las entidades que actúen como AR de Security Data Seguridad en Datos y Firma Digital.

La entidad que actúe como AR de Security Data Seguridad en Datos y Firma Digital podrá autorizar a una o varias personas como Operador de la AR para operar con el sistema informático de emisión de certificados de Security Data Seguridad en Datos y Firma Digital en nombre de la AR.

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, la AR podrá delegar estas funciones a otra entidad de confianza. Dicha entidad deberá tener una especial vinculación con la AR y una relación de proximidad con los suscriptores de los certificados que justifique la delegación. La entidad de confianza deberá firmar un acuerdo de colaboración con la AR en el

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	12

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.

2.3.5. Solicitante.

Solicitante es la persona física que, en nombre propio o en representación 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" dependiendo del tipo de certificado concreto.

2.3.6. Suscriptor.

El Suscriptor es la persona física 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. En general, el suscriptor de un certificado de Security Data Seguridad en Datos y Firma Digital será una persona jurídica (empresa privada, entidad pública, persona física), la identidad de la cual aparecerá en el propio certificado.

2.3.7. Firmante.

El Firmante es la persona que posee un dispositivo de creación de firma 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.

2.3.8. 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 física solicitante, sea representante legal o delegado autorizado, cuya identificación se incluirá en el certificado electrónico. El custodio tiene la obligación ineludible de mantener el control exclusivo de sus claves de acceso y dispositivos de firma.

El custodio reconoce que el uso de sus datos de activación y dispositivos de firma tiene los mismos efectos legales que una firma manuscrita, siendo responsable exclusivo de su uso y prohibiéndose expresamente la transferencia de claves a terceros.

2.3.9. Tercero que Confía en los Certificados.

Se entiende como tercero que confía en los certificados, a toda persona u organización que voluntariamente confía en un certificado emitido por Security Data. Para que la confianza sea válida, el tercero debe verificar siempre el estado de revocación del certificado a través de los mecanismos provistos por Security Data.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	13

Los certificados reconocidos emitidos por Security Data Seguridad en Datos y Firma Digital tienen carácter universal y están aceptados por la mayoría de los organismos públicos del estado ecuatoriano, como Ministerios, Secretarías, etc.

Las obligaciones y responsabilidades de Security Data Seguridad en Datos y Firma Digital con terceros que voluntariamente confíen en los certificados se limitarán a las recogidas en la DPC de Security Data Seguridad en Datos y Firma Digital.

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

2.4. USO DEL CERTIFICADO.

2.4.1. Usos Apropriados de los Certificados.

Los usos apropiados de los Certificados se regirán según lo definido en la DPC de Security Data.

2.4.2. Usos Prohibidos de los Certificados.

Los usos prohibidos de los Certificados se regirán según lo definido en la DPC de Security Data.

2.5. ADMINISTRACIÓN DE POLITICAS.

2.5.1. Organización que administra el Documento.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. es la entidad que administra y es autora de la presente Declaración de Políticas de Seguridad y demás documentos normativos.

2.5.2. Persona de Contacto.

Nombre:	SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.
Dirección:	Alonso de Torres y Edmundo Carvajal Centro Comercial "El Bosque" Oficinas Administrativas piso 1.
Domicilio:	Quito - Ecuador
Correo electrónico:	cto@securitydata.net.ec
Teléfono:	(02) 3922169
Página web:	www.securitydata.net.ec

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

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

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	14

2.5.4. Procedimientos de aprobación de la DPS.

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

Las versiones actualizadas y aprobadas de esta DPS, 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.

2.6. DEFINICIONES Y ACRÓNIMOS.

2.6.1. Definiciones.

ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones.

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

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.

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,

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	15

por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

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

Integridad: Propiedad que busca mantener los datos libres de modificaciones no autorizadas sin ser manipulada ni alterada salvo que este planificado hacerlo.

Disponibilidad: Calidad de la información de encontrarse accesible y utilizable en el momento, para las personas autorizadas en cada caso.

Seguridad de datos: Conjunto de medidas técnicas y organizativas necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Vulneración de la seguridad de los datos personales: Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

2.6.2. 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 Public (Public Key Infrastructure)

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	16

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), Atributo del Nombre Distintivo
CN:	Nombre Común (Common Name), Atributo del Nombre Distintivo
O:	Organización (Organization), Atributo del Nombre Distintivo
OU:	Unidad Organizacional (Organizational Unit), Atributo del Nombre Distintivo
SN:	Apellido (SurName), Atributo del Nombre Distintivo
ISO:	International Organization for Standardization
PKCS:	Public Key Cryptography Standards, Estándares PKI
UTF8:	Unicode Transformation Format – 8 bits.

3. Responsabilidades de Publicación y Repositorio.

3.1. REPOSITORIOS.

Declaración de Practicas de Seguridad: https://www.securitydata.net.ec/wp-content/downloads/Normativas/D_Practicas_Seguridad/declaracion_practicas_seguridad.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>

3.2. PROCEDIMIENTO DE APROBACIÓN.

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

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

3.3. TIEMPO O FRECUENCIA DE PUBLICACIÓN.

La presente DPS será revisada y si procede, actualizadas, anualmente o cuando se presente algún cambio.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	17

3.4. CONTROLES DE ACCESO A LOS REPOSITORIOS.

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

4. Identificación y Autenticación.

4.1. DENOMINACIÓN.

4.1.1. Tipos de Nombres.

Los tipos de nombres para los certificados se encuentran especificados en la DPC de Security Data.

4.1.2. Necesidad de que los nombres sean significativos.

Se seguirá según lo definido en la DPC de Security Data.

4.1.3. Reglas para interpretar varios formatos de nombres.

Las reglas se encuentran definidas en la DPC de Security Data.

4.1.4. Unicidad de los nombres.

Se seguirá según lo definido en la DPC de Security Data.

4.1.5. Reconocimiento, autenticación y función de las marcas.

No es aplicable.

4.2. VALIDACIÓN INICIAL DE LA IDENTIDAD.

Se seguirá el proceso definido en la DPC de Security Data.

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

Se seguirá el proceso definido en la DPC de Security Data.

4.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA SOLICITUD DE REVOCACIÓN.

Se seguirá el proceso definido en la DPC de Security Data.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	18

5. Requisitos Operacionales del Ciclo de Vida del Certificado.

5.1. SOLICITUD DEL CERTIFICADO.

El proceso de solicitud se realiza según lo definido en la DPC de Security Data.

5.2. TRAMITACIÓN DE LA SOLICITUD DEL CERTIFICADO.

El proceso de tramitación se realiza según lo definido en la DPC de Security Data.

5.3. EMISIÓN DEL CERTIFICADO.

El proceso de emisión se realiza según lo definido en la DPC de Security Data.

5.4. ACEPTACIÓN DEL CERTIFICADO.

El proceso de aceptación se realiza según lo definido en la DPC de Security Data.

5.5. USO DE PARES DE CLAVES Y CERTIFICADOS.

Los usos de las claves y certificados se rigen a lo definido en la DPC de Security Data.

5.6. RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVE.

No se contempla esta opción.

5.7. RENOVACIÓN CON CAMBIO DE CLAVE DEL CERTIFICADO.

El proceso de renovación se realiza según lo definido en la DPC de Security Data.

5.8. MODIFICACIÓN DEL CERTIFICADO.

No se contempla esta opción.

5.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO.

El proceso de revocación se realiza según lo definido en la DPC de Security Data.

5.10. SERVICIO DE ESTADO DE CERTIFICADO.

5.10.1. Características Operativas.

Según lo indicado en las DPC de Security Data.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	19

5.10.2. 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%.

5.10.3. Características Opcionales.

Sin estipulación.

5.11. FIN DE LA SUSCRIPCIÓN.

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

5.12. CUSTODIA Y RECUPERACIÓN DE CLAVES.

5.12.1. 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. En consecuencia, no es posible la recuperación de la clave privada del titular debido a que no existe copia alguna. La responsabilidad de la custodia de la clave privada es del titular y éste así lo acepta y reconoce.

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

No estipulado.

6. Controles de Instalaciones, Gestión y Operación.

6.1. 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:

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	20

- 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.

6.1.1. Ubicación física 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.

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.

6.1.2. 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.

6.1.3. Alimentación Eléctrica 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.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	21

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

6.1.4.Exposición al Agua.

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

6.1.5.Protección y Prevención de Incendios.

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

6.1.6.Sistema de Almacenamiento.

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

6.1.7.Eliminación de los Soportes de Información.

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

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

6.1.8.Seguridad de la Información Empresarial.

Se realizan respaldos diarios de la información.

6.2. CONTROLES DE PROCEDIMIENTO.

6.2.1.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

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	22

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 auditorias 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.
- 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.

6.2.2. 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.

6.2.3. 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.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	23

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

6.2.4. Roles 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.

6.3. CONTROLES DE PERSONAL.

6.3.1. 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.

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.

6.3.2. Procedimiento de Comprobación 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.

6.3.3. Requerimientos 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.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	24

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.

6.3.4. Requisitos y Frecuencia de Actualización de Formación.

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.

6.3.5. Frecuencia y Secuencia de Rotación de Tareas.

No se encuentra estipulado.

6.3.6. Sanciones por Actuaciones No Autorizadas.

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.

6.3.7. Requisitos de Contratación de Personal.

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.

6.3.8. Documentación Proporcionada 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

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	25

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.

6.4. PROCEDIMIENTOS DE REGISTRO DE AUDITORÍA.

6.4.1. Tipos de Eventos Registrados.

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

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de SECURITY DATA a través de la red.
- Intentos de accesos no autorizados a la red interna de SECURITY DATA.
- Intentos de accesos no autorizados al sistema de archivos.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de SECURITY DATA.
- Encendido y apagado de la aplicación de SECURITY DATA.
- 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.

6.4.2. Frecuencia de Procesado de Registros de Auditoría.

Se revisarán los logs de auditoría cada semana y en todo caso cuando se produzca una alerta del sistema motivado por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	26

6.4.3. 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.

6.4.4. Protección de los Registros.

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

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

Los dispositivos son manejados en todo momento por personal autorizado.

6.4.5. Procedimientos de Respaldo de los Registros de Auditoría.

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

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

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

6.4.6. Sistema de Recolección de Información de Auditoría.

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

6.4.7. Notificación de Eventos.

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.

En caso de una violación de seguridad que afecte datos personales o la integridad de la AC, Security Data notificará a la Autoridad de Protección de Datos y a ARCOTEL en un máximo de 72 horas, conforme al Art. 25 de la LOPDP.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	27

6.4.8. Análisis 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.

6.5. ARCHIVO DE REGISTRO.

6.5.1. Tipo de Eventos 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 auditoria.
- 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.

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

6.5.2. Periodo de Conservación de Registros.

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

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

6.5.3. 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.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	28

6.5.4. 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.

6.5.5. Requerimientos 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.

6.5.6. Sistema de Archivo de Información de Auditoría.

No estipulado.

6.5.7. 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.

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.

6.6. CAMBIO DE CLAVE DE LA AC.

6.6.1. 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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	29

6.6.2.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.

6.7. COMPROMISO Y RECUPERACIÓN ANTE DESASTRES.

6.7.1.Procedimientos de Gestión de Incidentes y Vulnerabilidades.

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.

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

En el caso de que tuviera lugar un incidente que alterara o corrompiera tanto recursos de hardware, software como datos, Security Data Seguridad en Datos y Firma Digital detendrá las operaciones normales hasta que se establezca un entorno seguro. De forma paralela, se llevará a cabo las revisiones pertinentes con el fin de identificar la causa y disponer las medidas necesarias para evitar futuras repeticiones.

En el caso de que los certificados digitales se emitan durante el periodo de incertidumbre y existe el riesgo de que estos certificados podrían verse comprometidas, a continuación, estos certificados serán revocados y los suscriptores serán notificados de la necesidad de volver a emitir sus certificados.

6.7.3.Procedimiento de Actuación ante la Vulnerabilidad de la Clave Privada de la AC.

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.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	30

6.7.4. 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.

6.8. TERMINACIÓN DE CA O RA.

6.8.1. 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.
- En caso de cese definitivo, Security Data coordinará con ARCOTEL la transferencia de los archivos y registros a otra Entidad de Certificación acreditada, para garantizar la continuidad de la validación de las firmas emitidas.

6.8.2. 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.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	31

7. Controles Técnicos de Seguridad.

7.1. GENERACIÓN E INSTALACIÓN DE PARES DE CLAVES.

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

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

7.2.1. 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.

7.2.2. 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.

7.2.3. 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.

7.2.4. 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 POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	32

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.

7.2.5. Archivo de la Clave Privada del Suscriptor.

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

Las claves privadas de los certificados internos que usan los distintos componentes del sistema de 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.

Security Data no genera, ni almacena, ni archiva en ningún caso la clave privada de firma del suscriptor. El control exclusivo de la clave privada reside únicamente en el suscriptor.

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

Existe un procedimiento interno de ceremonia de claves de la AC, 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.

7.2.7. 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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	33

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.

7.2.8. 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.

7.2.9. 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 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.

7.2.10. 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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	34

7.2.11. 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.

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

7.3.1. 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.

7.3.2. 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.

7.4. DATOS DE ACTIVACIÓN.

7.4.1. 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.

7.4.2. 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.

7.4.3. Otros aspectos de los datos de activación.

No estipulado.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	35

7.5. 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.
- 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.

7.5.1. Requerimientos Técnicos de Seguridad Específicos.

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.

7.5.2. 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.

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	36

7.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA.

7.6.1. 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.

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.

7.6.2. 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.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	37

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 con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de AC.

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.

7.6.3. 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.

7.7. 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.

 SECURITY DATA TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	38

7.8. 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.

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.

8. Perfiles de Certificados, CRL y OCSP.

8.1. PERFIL DEL CERTIFICADO.

Los perfiles de los certificados se encuentran definidos en la correspondiente PC y DPC.

8.2. PERFIL CRL.

El perfil de CRL se encuentra definido en la DPC de Security Data.

8.3. PERFIL OCSP.

El perfil de OCSP se encuentra definido en la DPC de Security Data.

9. Auditoría de Cumplimiento y Otras Evaluaciones.

9.1. FRECUENCIA DE LAS AUDITORIAS.

La frecuencia de las auditorías se realiza conforme lo definido en la DPC de Security Data.

9.2. CUALIFICACIÓN DEL AUDITOR.

El proceso se realiza conforme lo definido en la DPC de Security Data.

9.3. RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA.

El proceso se realiza conforme lo definido en la DPC de Security Data.

9.4. ASPECTOS CUBIERTOS POR LOS CONTROLES.

El proceso se realiza conforme lo definido en la DPC de Security Data.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	39

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

El proceso se realiza conforme lo definido en la DPC de Security Data.

9.6. COMUNICACIÓN DE RESULTADOS.

El proceso se realiza conforme lo definido en la DPC de Security Data.

10. Otros asuntos comerciales y legales.

10.1. TARIFAS.

La comunicación de las tarifas se realizará según lo definido en la DPC de Security Data.

10.2. RESPONSABILIDAD FINANCIERA.

Las coberturas del seguro se encuentran definidas en la DPC de Security Data.

10.3. CONFIDENCIALIDAD DE LA INFORMACIÓN EMPRESARIAL.

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

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

10.3.1. Alcance de la Información Confidencial.

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

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

 TU IDENTIDAD DIGITAL, EN UNA FIRMA.	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	40

10.3.2. Información No Confidencial.

La AC mantendrá como información no privada la siguiente:

- La contenida en la presente DPS, PC y DPC.
- Toda la información contenida en los certificados emitidos y listas de revocación de certificados (CRL), incluyendo toda la información que se pueda obtener de este tipo.
- Información de los certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) e información de los estados de certificados.
- Toda la información clasificada expresamente como "PÚBLICA".
- Información en relación a la revocación de un certificado.
- Cualquier otra información cuya publicidad sea impuesta normativamente

10.3.3. Deber de Proteger la Información Confidencial.

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

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

10.4. PRIVACIDAD DE LA INFORMACIÓN PERSONAL.

10.4.1. 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 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.

10.4.2. Información tratada como Privada.

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

10.4.3. Información No Calificada como Privada.

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

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	41

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

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

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

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

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

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

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

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

10.4.7. Otras circunstancias de revelación de información.

No se estipula.

10.5. 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.

10.6. DECLARACIONES Y GARANTÍAS.

Las declaraciones y garantías se encuentran definidas en la DPC de Security Data.

10.7. RENUNCIAS A GARANTÍAS.

Las renunciaciones a garantías se encuentran definidas en la DPC de Security Data.

10.8. LIMITACIONES DE RESPONSABILIDAD.

Las limitaciones de responsabilidad se encuentran definidas en la DPC de Security Data.

	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	42

10.9. INDEMNIZACIONES.

Las indemnizaciones se realizarán de acuerdo a lo definido en la DPC de Security Data.

10.10. PLAZO Y TERMINACIÓN.

10.10.1. Plazo.

Este documento de Declaración de Política de Seguridad y cualquier enmienda a este, entrarán en vigencia tras su publicación en la página web de SECURITY DATA, y permanecerán vigentes hasta que sea reemplazado por una versión más nueva.

10.10.2. Terminación.

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

10.11. AVISOS Y COMUNICACIONES INDIVIDUALES.

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.

10.12. ENMIENDAS.

Según lo definido en la DPC de Security Data.

10.13. RESOLUCIÓN DE DISPUTAS.

Según lo definido en la DPC de Security Data.

10.14. 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 Relacionados, emitida por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

10.15. CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE.

Los certificados emitidos bajo SECURITY DATA serán utilizados por los suscriptores y terceros

 SECURITY DATA <small>TU IDENTIDAD DIGITAL, EN UNA FIRMA.</small>	DECLARACIÓN DE POLÍTICAS DE SEGURIDAD	CÓDIGO	SD-ID-PE-15
		VERSIÓN	V2
		FECHA DE APROBACIÓN	18/02/2026
		PÁGINAS	43

que confían solo de acuerdo con las leyes y reglamentos de la jurisdicción en la que se utilizan o se basan.

10.16. DISPOSICIONES DIVERSAS.

Las disposiciones se encuentran definidas en la DPC de Security Data.

10.17. OTRAS DISPOSICIONES.

Sin estipulación.

11. Control de Aprobaciones.

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