SECURITY DATA
TU IDENTIDAD DIGITAL, EN UNA FIRMA.

# POLÍTICAS DE CERTIFICACIÓN REPRESENTANTE LEGAL

febrero 25

2026


www.securitydata.net.ec

info@securitydata.net.ec

392 2169 / 098 644 2122

## HISTORIAL DE VERSIONES

| VERSIÓN | DESCRIPCIÓN | FECHA | ELABORADO POR | REVISADO POR | APROBADO POR |
|---|---|---|---|---|---|
| V1 | Edición Inicial | 24/01/2011 | Coordinador Legal | Gerente Técnico | Gerente General |
| V2 | - | 31/03/2011 | Coordinador Legal | Gerente Técnico | Gerente General |
| V3 | - | 27/06/2011 | 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 | - | 15/12/2011 | Coordinador Legal | Gerente Técnico | Gerente General |
| V7 | - | 25/02/2015 | Coordinador Legal | Gerente Técnico | Gerente General |
| V8 | - | 25/06/2019 | Coordinador Legal | Gerente Técnico | Gerente General |
| V9 | - | 23/08/2022 | Coordinador Legal | Gerente Técnico | Gerente General |
| V10 | * Actualización general de la DPC conforme a la Normativa Técnica.<br>* Adaptación del documento a la norma RFC 3647. | 25/02/2026 | Coordinador del Sistema de Gestión | Chief Technology Officer (CTO)<br>Supervisor Legal | Gerente General |

## Contenido

# 1. Introducción.

## 1.1. DESCRIPCIÓN GENERAL.

El presente documento contempla la Política de Certificación (PC) de la Entidad de Certificación de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. para los certificados de Persona Jurídica para Representante Legal.

Esta PC específica y contempla lo establecido en la Declaración de Prácticas de Certificación (DPC) de la Entidad de Certificación de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. estableciendo un conjunto de reglas que indican los procedimientos seguidos por esta entidad en la prestación de sus servicios para la solicitud, identificación, aceptación, emisión, revocación de certificados digitales así como los límites de uso, el ámbito de aplicación y las características técnicas de este tipo de certificado.

Esta Política de Certificación (PC), junto con la DPC de la Entidad de Certificación de SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A., están dirigidas a cualquiera que confíe en este tipo de certificados.

## 1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO.

| | |
|---|---|
| **Nombre:** | Política de Certificación (PC) |
| **Versión:** | 10 |
| **Descripción:** | Política de Certificación de Persona Jurídica para Representante Legal. |
| **Fecha de emisión:** | 25 de febrero del 2026 |
| **Sitio Web:** | www.securitydata.net.ec |
| **Nombre de la empresa:** | Security Data Seguridad en Datos y Firma Digital S.A. |
| **Correo electrónico:** | info@securitydata.net.ec |
| **Dirección:** | Alonso de Torres y Av. Del Parque oficinas administrativas C8 |
| **Teléfono:** | 023922169 |

## 1.3. PARTICIPANTES DE LA PKI.

### 1.3.1. Entidad Acreditada (EA).

Security Data Seguridad en Datos y Firma Digital S.A. es un Entidad Acreditada (EA) que emite certificados reconocidos según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Security Data 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 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 S.A. está compuesto por diversas Autoridades de Certificación (en inglés CA o Certificate Authority) organizadas bajo una Jerarquía de Certificación.

### 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. Autoridad 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 S.A., 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 S.A.:

- Cualquier entidad de confianza que llegue a un acuerdo con Security Data Seguridad en Datos y Firma Digital S.A. para actuar como tercero en nombre de Security Data Seguridad en Datos y Firma Digital S.A.
- La propia Security Data Seguridad en Datos y Firma Digital S.A. directamente.

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; posteriormente la vinculación se formalizará mediante el respectivo registro del ente de control.

La entidad que actúe como Tercero Vinculado de Security Data Seguridad en Datos y Firma Digital S.A. 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 Seguridad en Datos y Firma Digital S.A. 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 S.A. 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 S.A. 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.

### 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 S.A.

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

Las obligaciones y responsabilidades de Security Data Seguridad en Datos y Firma Digital S.A. 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 del Certificado.

- Los certificados no tienen una limitante técnica, administrativa, financiera, etc. para su uso.
- El suscriptor podrá hacer uso del certificado de Firma Electrónica según lo establecido en esta DPC, en el contrato de prestación de servicios que suscriba con SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, y la PC.
- Los usos autorizados de los Certificados emitidos por SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL pueden estar especificados en cada tipo de certificado.
- Si el certificado del suscriptor en el período de vigencia se encontrara comprometido, es decir su clave privada, deberá iniciar el procedimiento de revocación como se lo menciona en la DPC de Security Data.
- Los certificados deben usarse en conformidad a lo que dice la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos para el uso de claves y certificados.
- Los certificados de Representación Legal ante las Administración Pública, se limita el uso a aquellos que le permitan los poderes de representación.
- El certificado de firma electrónica emitido por SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL al suscriptor, deberá ser utilizado tal y como son suministrados. Queda prohibida cualquier alteración del certificado por parte del usuario.
- Los certificados de firma electrónica no podrán ser utilizados para acciones ilícitas, de acuerdo con lo establecido en la legislación ecuatoriana.
- Los certificados de firma electrónica presentan las siguientes garantías:

- Autenticidad: La información del documento y su firma electrónica se corresponden indubitablemente con la persona que ha firmado.
- 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 propósito del uso de las llaves de la AC es establecido en el estándar x509 v3.
- El certificado digital raíz sólo puede utilizarse para la identificación de la propia autoridad de certificación raíz y para la distribución de su clave pública de forma segura.

### 1.4.2. Usos prohibidos del Certificado.

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

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

Se considerará que se hace un uso indebido de un Certificado cuando éste sea utilizado para realizar operaciones no autorizadas según las Políticas de Certificados aplicables a cada uno de los Certificados, y los contratos con sus suscriptores, consecuencia de esto, Security Data podrá revocar el certificado y dar por terminado el contrato.

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

## 1.5. ADMINISTRACIÓN DE POLÍTICAS.

### 1.5.1. Organización que administra el documento.

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

### 1.5.2. Persona de contacto.

| | |
|---|---|
| **Persona de 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 |

### 1.5.3. Persona que determina la idoneidad de las Políticas de Certificación.

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. Procedimientos de aprobación de las Políticas de Certificación.

Las Políticas de Certificación serán revisadas y si procede la actualización, se lo realizará anualmente o cuando se presente algún cambio.

Las Políticas de Certificación de Security Data Seguridad en Datos y Firma Digital S.A. serán aprobadas por el Gerente General una vez se haya revisado y corroborado que se cumple con los requisitos de ley y su cumplimiento.

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

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

## 1.6. DEFINICIONES Y ACRÓNIMOS.

### 1.6.1. Definiciones.

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

**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, 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.

**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.

**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.

### 1.6.2. 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**: Light weight 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 (Dinstinguished Name)
**C**: País (Country)
**CN**: Nombre Común (Common Name)
**O:** Organización (Organization)
**OU**: Unidad Organizacional (Organizational Unit
**SN**: Apellido (SurName)
**ISO**: International Organizational for Standarization
**PKCS**: Public Key Cryptography Standars, Estándares PKI
**UTF8**: Unicode Transformation Format – 8 bits.

## 2. Responsabilidades de Publicación y Repositorio.

### 2.1. REPOSITORIOS.

Los repositorios se encuentran en la página web de Security Data Seguridad en Datos y Firma Digital S.A., los cuales están referenciados en la siguiente URL https://repositorio.securitydata.net.ec/security1/ .

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

Política de Certificación de Representante Legal:
https://www.securitydata.net.ec/wp-content/downloads/Normativas/P_de_Certificados/Politicas%20de%20Certificado%20Representante%20Legal.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

Consulta de certificados:
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.

## 2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN.

Tanto la Declaración de Prácticas de Certificación como las Políticas de Certificación, 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.

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

Security Data Seguridad en Datos y Firma Digital no está obligada a publicar los certificados emitidos en un repositorio de acceso público. Sin embargo, con el fin de mejorar los servicios a los clientes, Security Data Seguridad en Datos y Firma Digital podría ofrecer servicios de Directorio y de búsqueda y descarga de algunos certificados emitidos bajo su jerarquía de certificación.

## 2.3. TIEMPO O FRECUENCIA DE PUBLICACIÓN.

La AC publicará la lista de certificados emitidos de forma inmediata, posterior a su emisión.

La AC Raíz emitirá una Lista de ACs Revocadas (ARL) como mínimo cada seis meses, o extraordinariamente, cuando se produzca la revocación de un certificado de autoridad. Cada AC Subordinada emitirá una Lista de Certificados Revocados (CRL) diariamente, y de forma extraordinaria, cada vez que se suspenda o revoque un certificado.

Las CRL de la AC Subordinada se actualizará y publicará cada 24 horas, y de manera extraordinaria cuando se produzca la revocación o suspensión de un certificado.

Security Data Seguridad en Datos y Firma Digital revisará y si procede, actualizará la DPC y PC anualmente, o cuando se presente algún cambio y publicará de forma inmediata cualquier modificación en las políticas y prácticas de certificación.

### 2.4. CONTROLES DE ACCESO A LOS REPOSITORIOS.

Las Políticas de Certificación, la Declaración de Prácticas de Certificación, las Condiciones Generales de Contratación, los certificados de AC y las listas de certificados revocados (CRL) se publicarán en repositorios de acceso público sin control de acceso.

Los certificados emitidos podrán publicarse en repositorios públicos o de acceso restringido según las necesidades. Los servicios de validación por el protocolo OCSP y de sellado de tiempo por el protocolo TSP serán servicios de acceso restringido y de pago.

La administración de los repositorios estará a cargo de Security Data Seguridad en Datos y Firma Digital S.A.

## 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.

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.

## 3.2. VALIDACIÓN DE IDENTIDAD INICIAL.

Para la validación de identidad de Persona Jurídica como Representante Legal, 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.

### 3.2.2. Autenticación de la identidad de la organización.

Los Certificados de Organización son certificados de firma electrónica emitidos a favor de una Persona Jurídica, cuyo titular puede ser una empresa, organización o entidad de la Administración Pública. Estos certificados permiten identificar de manera electrónica a la persona jurídica como sujeto suscriptor y son reconocidos conforme a la normativa vigente.

- Certificados de Representante Legal: Son certificados reconocidos que identifican al suscriptor como una persona jurídica y al firmante como representante legal de dicha organización.

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 de la persona jurídica deberá presentar la cédula de identidad, pasaporte u otro medio reconocido en derecho que le identifique.

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

### 3.2.3. Autenticación de la identidad individual.

No es aplicable.

### 3.2.4. Información de suscriptor no verificada.

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

### 3.2.5. Validación de la autoridad.

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

En el caso de certificados emitidos a personas jurídica como representante legal, 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.

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

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

### 3.2.6. Criterios de interoperabilidad.

Security Data emite certificados de 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 PARA SOLICITUDES DE 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, 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 DE IDENTIDAD INICIAL, 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.

## 4. Requisitos operacionales del ciclo de vida del certificado.

### 4.1. SOLICITUD DEL CERTIFICADO.

### 4.1.1. Quién puede presentar una solicitud de certificado.

La solicitud de un certificado de firma electrónica la puede presentar o ser tramitada por una persona física en representación de una organización.

Security Data solo admite solicitud de emisión de certificado tramitada por una persona física, bajo relación de dependencia, 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 S.A. para gestionar la solicitud del certificado, ya sea por medio de la página web de la AC, presencialmente, canales de comunicación de la AC 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 y la organización.

- 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 DPC.

La Autoridad 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 para certificados de representante legal.

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, en caso de que los servicios se hayan caído, el operador de registro pedirá al solicitante su documento de identificación y el registro único de contribuyente (RUC) para realizar la verificación de la identidad de forma manual. Así mismo, se revisarán todos los requisitos habilitantes de representante legal. 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 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 proceso de inscripción de manera segura, confiable y conforme a los estándares técnicos y regulatorios aplicables.

## 4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADO

### 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.

Los documentos que se verificaran dependiendo del tipo de firma que el suscriptor solicitará será la siguiente:

**Personas Jurídica (Representante Legal):**

- Se realizará un proceso de validación de la identidad del solicitante según lo mencionado en el apartado VALIDACIÓN DE IDENTIDAD INICIAL para ciudadanos ecuatorianos, para el caso de extranjeros se solicitará el pasaporte, este no realizará validación biométrica, se le solicitará video que permita confirmar su identidad y voluntad respecto a la obtención o renovación del certificado, conforme a los procedimientos internos establecidos por Security Data.
- La autoridad de certificación validará ante el SRI el RUC y almacenará una captura del estado del mismo, en caso de que la página del SRI no se encuentre disponible, el certificado no se otorga hasta que se realice la validación manual del RUC.
- Copia legible del nombramiento o poder, que conceda la representación legal con su debida inscripción cuando corresponda, o registro de directivas según el caso del representante legal en caso de Personas Jurídicas.
- Copia de constitución, estatutos o documento de creación según corresponda de la Empresa solicitante.

### 4.2.2. Aprobación o rechazo de 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, si la solicitud es realizada en línea, 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, en caso de no estar disponibles los servicios, el operador de registro deberá realizar estas verificaciones de forma manual con los documentos habilitantes emitidos por las entidades competentes.

En caso de personas jurídicas el operador de registro y tercer vinculado deberán verificar todos los documentos habilitantes a la representación legal.

Si la información no es correcta, el operador de registro negará la solicitud comunicando el motivo y así mismo, 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 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 de forma 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 CA durante la emisión del certificado.

Security Data genera certificados de 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.

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 soporte 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

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.

**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 cliente 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**

- La AC notificará mediante correo electrónico al suscriptor, que el certificado 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 suscriptor haya aceptado términos y condiciones al momento de la descarga y 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 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 de la AC.

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

No se estipula

## 4.5. USO DE PARES DE CLAVES Y CERTIFICADOS.

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

El uso de la clave privada y el certificado están sujetos a los términos del acuerdo del suscriptor y lo especificado en el presente documento y las DPC, el uso de una clave privada sólo se permite después de que el suscriptor ha aceptado el certificado 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 Seguridad en Datos y Firma Digital 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.
- **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.

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

Los terceros que confían en los certificados podrán utilizar los certificados para aquello que

establece la DPC y la presente Política de Certificación.

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

## 4.6. RENOVACIÓN 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. Circunstancia para la renovación 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:

- 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.

### 4.6.2. Quien puede solicitar la renovación.

La renovación del certificado de firma electrónica puede ser solicitado por el titular o un tercero debidamente autorizado y los requisitos que debe reunir para certificados de persona jurídica para representante legal se encuentran especificados en el apartado *Realización de funciones de identificación y autenticación*.

### 4.6.3. Tramitación de solicitudes de renovación de certificados.

La tramitación de la renovación de certificados se la realizará mediante los medios autorizados por la AC para la realización de emisión de certificados, el solicitante deberá contactar con Security Data Seguridad en Datos y Firma Digital, estos medios pueden ser online mediante la página web, medios de comunicación autorizados o de forma presencial.

La AC receptará la solicitud y la registrará para la posterior verificación de los datos, el suscriptor deberá contar con lo siguiente:

- Documentación necesaria para presentar para la tramitación de su solicitud y para verificar la identidad del suscriptor, los requisitos se los encontrará en el presente documento en el apartado TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADO,

Realización de funciones de identificación y autenticación

- 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.

La validación de la identidad se la realizará en base al apartado VALIDACIÓN DE IDENTIDAD INICIAL del presente documento.

### 4.6.4. 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 para que el suscriptor proceda a realizar la renovación de su certificado.

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

Si el suscriptor procede a la renovación, cuando se haya emitido el nuevo certificado la AC notificará a este por correo electrónico la emisión del certificado para que proceda a la descarga.

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

El certificado se aceptará en el momento que el suscriptor haya aceptado términos y condiciones al momento de la descarga y 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.

### 4.6.6. Publicación del certificado de renovación 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.

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

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

## 4.7. CAMBIO DE CLAVE DEL CERTIFICADO.

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

Se podrá renovar la clave del certificado bajo las siguientes circunstancias:

- 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 certificación de una nueva clave pública puede ser solicitado por el titular o un tercero debidamente autorizado y los requisitos que debe reunir dependerán del tipo de certificado solicitado.

### 4.7.3. Procesamiento de solicitudes de renovación de claves de certificados.

Proceso de renovación, que se efectuará del mismo modo que la emisión de un nuevo certificado, ya que el suscritor 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 del mismo.

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.

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

Cuando se haya emitido el nuevo certificado la AC notificará al suscriptor la emisión del nuevo certificado para que proceda a la descarga, esta notificación se la hará por correo electrónico.

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

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 suscriptor haya aceptado términos y condiciones al momento de la descarga y 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.

### 4.7.6. 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 de certificados por parte de la CA a otras entidades.

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

## 4.8. MODIFICACIÓN DEL CERTIFICADO.

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 acercase a las oficinas de la AR con las respectivas evidencias para la corrección o contactar a la entidad por los medios aprobados para la corrección de los datos.

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 suscriptor haya aceptado términos y condiciones al momento de la descarga y 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 podrá ser publicado en los repositorios de certificados publicados en la página web de Security Data.

### 4.8.7. Notificación de la emisión de certificados por parte de 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. Circunstancias de Revocación.

Un certificado podrá ser revocado debido a las siguientes causas:

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

- 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 Tercero 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 autorizados, por un tercero, de la clave privada del suscriptor.
  - El uso irregular del certificado por el suscriptor o firmante.
  - El incumplimiento por parte del suscriptor o firmante de las normas de uso del certificado expuestas en la presente DPC o en el instrumento jurídico vinculante entre Security Data Seguridad en Datos y Firma Digital y el suscriptor.

- 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 las DPC o en el instrumento jurídico vinculante entre Security Data Seguridad en Datos y Firma Digital y el suscriptor.

- 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, responsabilidad 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.

- 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.
- Sucesión: Herederos legítimos en caso de fallecimiento (adjuntando documentación).
- Mandato Judicial: Orden expresa de autoridad competente.
- La EC que emitió el certificado.
- La ER a través del cual de emitió el certificado.
- 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 AC.
- Los operadores autorizados de la AR o del Tercero Vinculado a la que pertenece el suscriptor del certificado.

### 4.9.3. Procedimiento para la solicitud de revocación.

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 Jurídica:** El titular, en su calidad de 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.

II. **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:

- 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.

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 CRL.

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.

### 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.
- 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 período 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.

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

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.

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

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.

### 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 y, por lo tanto, no presta servicio de recuperación de claves.

#### 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.

#### 5.1.1. Ubicación del sitio y construcción.

Los controles de ubicación del sitio y construcción se aplicarán según lo definido en la DPC y la Declaración de Política de Seguridad (DPS).

#### 5.1.2. Acceso Físico.

Los controles de acceso físico se aplicarán según lo definido en la DPC y DPS.

#### 5.1.3. Energía y Aire Acondicionado.

Los controles de energía y aire acondicionado se aplicarán según lo definido en la DPC y DPS.

#### 5.1.4. Exposición al Agua.

Los controles de exposición al agua se aplicarán según lo definido en la DPC y DPS.

#### 5.1.5. Protección y Prevención de Incendios.

Los controles de protección y prevención de incendios se aplicarán según lo definido en la DPC y DPS.

#### 5.1.6. Sistema de Almacenamiento.

Los controles para el sistema de almacenamiento se aplicarán según lo definido en la DPC y DPS.

### 5.1.7. Eliminación de los Soportes de Información.

Los controles para la eliminación de residuos se aplicarán según lo definido en la DPC y DPS.

### 5.1.8. Copia de Seguridad Externa.

Los controles para las copias de seguridad externa se aplicarán según lo definido en la DPC y DPS.

## 5.2. CONTROLES DE PROCEDIMIENTO.

### 5.2.1. Roles de Confianza.

Los controles para la definición de roles de confianza se aplicarán según lo definido en la DPC y DPS.

### 5.2.2. Número de personas necesarias por tarea.

Los controles para la definición del número de personas necesarias por tarea se aplicarán según lo definido en la DPC y DPS.

### 5.2.3. Identificación y autenticación por cada rol.

Los controles para la identificación y autenticación para cada rol se aplicarán según lo definido en la DPC y DPS.

### 5.2.4. Roles que requieren separación de funciones.

Los controles para la definición funciones que requieren separación de funciones se aplicarán según lo definido en la DPC y DPS.

## 5.3. CONTROLES DE PERSONAL.

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

Los requisitos se encuentran definidos en la DPC y DPS de Security Data.

### 5.3.2. Procedimiento de Comprobación de Antecedentes.

El procedimiento para la comprobación de antecedentes se aplicará según lo definido en la DPC y DPS.

### 5.3.3. Requerimientos de Formación.

Los controles se aplicarán según lo definido en la DPC y DPS.

### 5.3.4. Requisitos y Frecuencia de Actualización de Formación.

Se aplicarán según lo definido en la DPC y DPS.

### 5.3.5. Frecuencia y Secuencia de Rotación de Tareas.

Se aplicarán según lo definido en la DPC y DPS.

### 5.3.6. Sanciones por Actuaciones No Autorizadas.

El proceso para la ejecución de sanciones se seguirá según lo definido en la DPC y DPS.

### 5.3.7. Requisitos de Contratación de Personal.

Se seguirá según lo definido en la DPC y DPS.

### 5.3.8. 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 políticas, procedimientos y formatos de todos los procesos de la AC, teniendo en cuenta, y sin limitarse a 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.

Los tipos de eventos se encuentran definidos en la DPC y DPS.

### 5.4.2. Frecuencia de Procesado de Registros de Auditoría.

La frecuencia de procesado se encuentra definido en la DPC y DPS.

### 5.4.3. Periodo de Conservación de los Registros de Auditoría.

El periodo de conservación se encuentra definido en la DPC y DPS.

### 5.4.4. Protección de los Registros.

La protección de los registros se encuentra definido en la DPC y DPS.

### 5.4.5. Procedimientos de Respaldo de los Registros de Auditoría.

Los procedimientos de respaldo se encuentran definidos en la DPC y DPS.

### 5.4.6. Sistema de Recolección de Información de Auditoría.

Se seguirá según lo definido en la DPC y DPS.

### 5.4.7. Notificación de Eventos.

La notificación de eventos se realizará según lo definido en la DPC y DPS.

### 5.4.8. Análisis de Vulnerabilidades.

El análisis se realizará según lo definido en la DPC y DPS.

## 5.5. ARCHIVO DE REGISTRO.

### 5.5.1. Tipo de Eventos Archivados.

Según lo definido en la DPC y DPS.

### 5.5.2. Periodo de Conservación de Registros.

El periodo de conservación de registros se encuentra definido en la DPC y DPS.

### 5.5.3. Protección del Archivo.

La protección del archivo se encuentra definido en la DPC y DPS.

### 5.5.4. Procedimientos de Copia de Seguridad del Archivo.

Los procedimientos se seguirán según lo definido en la DPC y DPS.

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

Los requerimientos se encuentran definidos en la DPC y DPS.

### 5.5.6. Sistema de Archivo de Información de Auditoría.

Los controles se encuentran definidos en la DPC y DPS.

### 5.5.7. Procedimientos para obtener y verificar información de archivo.

Los procedimientos se encuentran definidos en la DPC y DPS.

### 5.6. CAMBIO DE CLAVE DE LA AC.

El proceso para cambio de clave se encuentra definido en la DPC de Security Data.

### 5.7. COMPROMISO Y RECUPERACIÓN ANTE DESASTRES.

#### 5.7.1. Procedimientos de Gestión de Incidentes y Vulnerabilidades.

El procedimiento se encuentra definido en la DPC y DPS.

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

Se seguirá según lo definido en la DPC y DPS.

#### 5.7.3. Procedimiento de Actuación ante la Vulnerabilidad de la Clave Privada de la AC.

Se seguirá según lo definido en la DPC y DPS.

#### 5.7.4. Continuidad del Negocio después de un desastre.

Se seguirá según lo definido en la DPC y DPS.

### 5.8. TERMINACIÓN DE CA O RA.

Se seguirá el procedimiento según lo definido en la DPC y DPS.

## 6. Controles Técnicos de Seguridad.

### 6.1. GENERACIÓN E INSTALACIÓN DE PARES DE CLAVES.

#### 6.1.1. Generación de Pares de Claves.

La generación del par de claves se realiza según lo definido en la DPC.

#### 6.1.2. Entrega de Clave Privada al Suscriptor.

La entrega de la clave privada al suscriptor se la realiza de acuerdo a lo definido en la DPC.

#### 6.1.3. Entrega de Clave Pública al emisor del Certificado.

La entrega de la clave pública se la realiza de acuerdo a lo definido en la DPC.

#### 6.1.4. Entrega de Clave Pública de CA a partes Confiables.

La entrega de la clave pública se la realiza de acuerdo a lo definido en la DPC.

### 6.1.5. Tamaños de Clave.

Se encuentra definido en la DPC.

### 6.1.6. Generación de Parámetros de Clave Pública y control de calidad.

El procedimiento se realiza de acuerdo a lo definido en la DPC.

### 6.1.7. Fines de uso de la Clave.

Los fines de uso se encuentran definidos en la DPC.

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

### 6.2.1. Estándares para los Módulos Criptográficos.

Los estándares se encuentran definidos en la DPC y DPS.

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

Según lo definido en la DPC y DPS.

### 6.2.3. Custodia de la Clave Privada.

Según lo definido en la DPC y DPS.

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

Según lo definido en la DPC y DPS.

### 6.2.5. 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.

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

La transferencia se la realiza según a lo definido en la DPC y DPS.

### 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 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.

### 6.2.8. Método de Activación de la Clave Privada.

El proceso se realiza según a lo definido en la DPC y DPS.

### 6.2.9. Método de Desactivación de la Clave Privada.

El proceso se realiza según a lo definido en la DPC y DPS.

### 6.2.10. Método de Destrucción de la Clave Privada.

Para la destrucción de la clave privada, se seguirá el proceso definido en la DPC y DPS.

### 6.2.11. Clasificación del módulo criptográfico.

Según lo definido en la DPC y DPS.

## 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.
- 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. Requerimientos Técnicos de Seguridad Específicos.

Los requerimientos técnicos necesarios, se encuentran especificados en la DPC y DPS de Security Data.

#### 6.5.2. Clasificación de la Seguridad Informática.

La clasificación se encuentra especificada en la DPC y DPS de Security Data.

### 6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA.

#### 6.6.1. Controles de Desarrollo de Sistemas.

Los controles necesarios se encuentran definidos en la DPC y DPS de Security Data.

#### 6.6.2. Controles de Gestión de Seguridad.

Los controles necesarios se encuentran definidos en la DPC y DPS de Security Data.

#### 6.6.3. Controles de Seguridad del Ciclo de Vida.

Los controles necesarios se encuentran definidos en la DPC y DPS de Security Data.

### 6.7. CONTROLES DE SEGURIDAD DE LA RED.

Los controles necesarios se encuentran definidos en la DPC y DPS de Security Data.

### 6.8. SELLADO DE TIEMPO.

Según lo definido en la DPC de Security Data.

## 7. Perfiles de Certificados, CRL y OCSP.

### 7.1. PERFIL DEL CERTIFICADO.

Los certificados de firma electrónica permiten identificar de manera inequívoca al titular y vincular su identidad con una clave criptográfica, posibilitando la firma de documentos electrónicos con garantías de autenticidad, integridad y no repudio, conforme a la normativa vigente.

Security Data en el marco de su servicio de certificados de firma electrónica, emite certificados de Persona Jurídica como Representante Legal.

Estos certificado puede ser emitido en los siguientes soportes:

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

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

**a. Certificado de Representante Legal en Archivo:**

| Campo | en Archivo | Oblig. | Crit. | Observaciones |
|---|---|---|---|---|
| De Persona Natural | Autenticación y Firma | | | OID 1.3.6.1.4.1.oid_AC.2.3.1 |
| **1. Basic estructure** | | | | |
| **1.1. Version** | "2" | SI | | El literal "2" corresponde a la versión 3. X.509 v3 |
| **1.2. Serial Number** | Establecido automáticamente por la AC Número identificativo único del certificado. | SI | | No puede ser un número negativo ni 0. |
| **1.3. Signature Algorithm** | | SI | | |
| 1.3.1. Algorithm | SHA-256 with RSA Signature | SI | | 1.2.840.113549.1.1.11 |
| 1.3.2. Parameters | No aplicable | No | | |
| **1.4. Issuer** | | SI | | |
| 1.4.1. Country Name ( C ) | Código del País "EC" (ISO 3166) | SI | | OID 2.5.4.6 |
| 1.4.2. Organization Name(O) | Nombre de la AC Subordinada "Organización" | SI | | OID 2.5.4.10 |
| 1.4.3. Locality Name (L) | Localidad de la AC Subordinada (Ciudad) Ej. QUITO | SI | | OID 2.5.4.7 |
| 1.4.5. Common Name (CN) | Nombre de la AC Subordinada | SI | | OID 2.5.4.3 |
| 1.4.6. Organizational Unit Name (OU) | Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA | No | | OID 2.5.4.11 |
| **1.5. Validity** | | SI | | |
| 1.5.1. Not Before | Fecha de inicio de validez | SI | | YYMMDDHHMMSSZ |
| 1.5.2. Not After | Fecha de expiración | SI | | YYMMDDHHMMSSZ |
| **1.6. Subject** | | SI | | |
| 1.6.1. Country Name (C) | País donde reside la Persona Jurídica (Pública o Privada) "EC" (ISO 3166) | SI | | OID 2.5.4.6 |
| 1.6.2. Locality Name (L) | Localidad de la Persona Jurídica (Pública o Privada) (Ciudad) ej. QUITO | SI | | OID 2.5.4.7 |
| 1.6.3. Organization Name (O) | Persona Jurídica (Pública o Privada) de la cual es Representante Legal o Apoderado el Signatario | SI | | OID 2.5.4.10 |
| 1.6.4. Organization Identifier | Número de Registro Único de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Signatario "VAT(CÓDIGO_PAIS)-RUC Ej. VATEC-1716151413001 | No | | OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio |
| 1.6.5. Title | Se especificará el nombre del título o el puesto (cargo) que el Signatario ocupa. Ej. REPRESENTANTE LEGAL O APODERADO | SI | | OID 2.5.4.12 |

| | | | | |
|---|---|---|---|---|
| 1.6.6. Surname | Apellidos del Signatario (como consta en el documento oficial) | SI | | OID 2.5.4.4 |
| 1.6.7. Given Name | Nombres del Signatario (como consta en el documento oficial) | SI | | OID 2.5.4.42 |
| 1.6.8. Serial Number | Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611 | SI | | OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1 |
| 1.6.9. Common Name (CN) | Nombres y Apellidos del Signatario | SI | | OID 2.5.4.3 |
| **1.7. Subject Public Key Info** | | SI | | |
| 1.7.1. AlgorithmIdentifier | | | | |
| 1.7.1.1. Algorithm | RSA encryption | SI | | OID 1.2.840.113549.1.1.1 |
| 1.7.1.2. Parameters | No aplicable | NO | | |
| 1.7.2. SubjectPublicKey | Clave pública del Signatario | SI | | Acorde ETSI TS 119 312 |
| **2. Extensions** | | | | |
| **2.1. Authority Key Identifier** | Identificador de la clave del Issuer | No | NO | OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es Obligatorio siempre y cuando la clave pública de la AC se distribuya en formato de certificado "AUTOFIRMADO" |
| 2.1.1. KeyIdentifier | | No | | Derivado de la clave pública |
| **2.2. Subject Key Identifier** | Identificador de la clave del Subject | SI | NO | OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2) |
| 2.2.1. KeyIdentifier | | SI | | Derivado de la clave pública |
| **2.3. Key Usage** | | SI | SI | OID 2.5.29.15 |
| 2.3.1. Digital Signature | Seleccionado “1” | SI | | |
| 2.3.2. Content commintment | Seleccionado “1” | SI | | |
| 2.3.3. Key Encipherment | Seleccionado “1” | SI | | |
| 2.3.4. Data Encipherment | No seleccionado. “0” | | | |
| 2.3.5. Key Agreement | No seleccionado. “0” | | | |
| 2.3.6. Key Certificate Signature | No seleccionado. “0” | | | |
| 2.3.7. CRL Signature | No seleccionado. “0” | | | |
| 2.3.8. Encipher Only | No seleccionado. “0” | | | |
| 2.3.9. Decipher Only | No seleccionado. “0” | | | |
| **2.4. Certificate Policies** | | SI | NO | OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2) |
| 2.4.1. Policy Information | | SI | | |
| 2.4.1.1. Policy Identifier | 1.3.6.1.4.1.oid_AC.2.3.1 | SI | | Identificador de la política de la AC |
| 2.4.1.2. Policy Qualifiers | | SI | | |
| 2.4.1.1.1 CPS URI | (https://www.repo_example.com/dpc/) | SI | | OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada |
| 2.4.1.1.2. User Notice/Explicit text | “CERTIFICADO DE REPRESENTANTE LEGAL EN ARCHIVO" | SI | | OID 1.3.6.1.5.5.7.2.2 Texto indicativo |

| | | | | |
|---|---|---|---|---|
| **2.5. Subject Alternative Names** | | NO | NO | OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2) |
| 2.5.1. rfc822Name | Correo electrónico del Signatario "nombreapellido@example.com.ec" | SI | | |
| **2.6. Extended Key Usage** | | SI | NO | OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2) |
| 2.6.1. clientAuth | Presente (1.3.6.1.5.5.7.3.2) | SI | | Transport Layer Security (TLS) World Wide Web (WWW) client authentication |
| 2.6.2. Email protection | Presente (1.3.6.1.5.5.7.3.4) | NO | | Sólo se activa si se incluye el correo electrónico del Signatario |
| **2.7. cRLDistributionPoint** | | SI | NO | OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2) |
| 2.7.1. distributionPoint | (http://crl1.example.com/example1subordinada.crl) | SI | | http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETFRFC 4516 [4] scheme |
| 2.7.2. distributionPoint | (http://crl2.example.com/example2subordinada.crl) | No | | http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETFRFC 4516 [4] scheme |
| **2.8. Authority Information Access** | | SI | NO | OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2) |
| 2.8.1. Access Description | | SI | | |
| 2.8.1.1. Access Method | id-ad-ocsp | Si | | OID 1.3.6.1.5.5.7.48.1 |
| 2.8.1.1.1 Access Location | (http://ocsp1.example.com/ocsp/) | Si | | URL de acceso al OCSP(http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5] |
| 2.8.1.1.2. Access Location | (http://ocsp2.example.com/ocsp/) | No | | URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5] |
| 2.8.2. Access Description | | No | | No es Obligatorio siempre y cuando incluya la ubicación de acceso al OCSP |
| **2.9. Basic Constraints** | | SI | SI | OID 2.5.29.19 |
| 2.9.1. cA | FALSE | SI | | |

### b. Certificado de Representante Legal en DSCF:

| Campo | en Dispositivo Seguro de Creación de Firma DSCF | Oblig. | Crit. | Observaciones |
|---|---|---|---|---|
| **De Persona Natural** | **Autenticación y Firma** | | | **OID 1.3.6.1.4.1.oid_AC.2.3.2** |
| **1. Basic estructure** | | | | |
| **1.1. Version** | "2" | SI | | El literal "2" corresponde a la versión 3. X.509 v3 |
| **1.2. Serial Number** | Establecido automáticamente por la AC Número identificativo único del certificado. | SI | | No puede ser un número negativo ni 0. |
| **1.3. Signature Algorithm** | | SI | | |
| 1.3.1. Algorithm | SHA-256 with RSA Signature | SI | | 1.2.840.113549.1.1.11 |
| 1.3.2. Parameters | No aplicable | No | | |
| **1.4. Issuer** | | SI | | |
| 1.4.1. Country Name ( C ) | Código del País "EC" (ISO 3166) | SI | | OID 2.5.4.6 |

| | | | | |
|---|---|---|---|---|
| 1.4.2. Organization Name(O) | Nombre de la AC Subordinada "Organización" | SI | | OID 2.5.4.10 |
| 1.4.5. Common Name (CN) | Nombre de la AC Subordinada | SI | | OID 2.5.4.3 |
| 1.4.6. Organizational Unit Name (OU) | Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA | No | | OID 2.5.4.11 |
| **1.5. Validity** | | SI | | |
| 1.5.1. Not Before | Fecha de inicio de validez | SI | | YYMMDDHHMMSSZ |
| 1.5.2. Not After | Fecha de expiración | SI | | YYMMDDHHMMSSZ |
| **1.6. Subject** | | SI | | |
| 1.6.1. Country Name (C) | País donde reside la Persona Jurídica (Pública o Privada) "EC" (ISO 3166) | SI | | OID 2.5.4.6 |
| 1.6.2. Locality Name (L) | Localidad de la Persona Jurídica (Pública o Privada) (Ciudad) ej. QUITO | SI | | OID 2.5.4.7 |
| 1.6.3. Organization Name (O) | Persona Jurídica (Pública o Privada) de la cual es Representante Legal o Apoderado el Signatario | SI | | OID 2.5.4.10 |
| 1.6.4. Organization Identifier | Número de Registro Único de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Signatario "VAT(CÓDIGO_PAIS)-RUC Ej. VATEC-1716151413001 | No | | OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio |
| 1.6.5. Title | Se especificará el nombre del título o el puesto (cargo) que el Signatario ocupa. Ej. REPRESENTANTE LEGAL O APODERADO | SI | | OID 2.5.4.12 |
| 1.6.6. Surname | Apellidos del Signatario (como consta en el documento oficial) | SI | | OID 2.5.4.4 |
| 1.6.7. Given Name | Nombres del Signatario (como consta en el documento oficial) | SI | | OID 2.5.4.42 |
| 1.6.8. Serial Number | Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611 | SI | | OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1 |
| 1.6.9. Common Name (CN) | Nombres y Apellidos del Signatario | SI | | OID 2.5.4.3 |
| **1.7. Subject Public Key Info** | | SI | | |
| 1.7.1. AlgorithmIdentifier | | | | |
| 1.7.1.1. Algorithm | RSA encryption | SI | | OID 1.2.840.113549.1.1.1 |
| 1.7.1.2. Parameters | No aplicable | NO | | |
| 1.7.2. SubjectPublicKey | Clave pública del Signatario | SI | | Acorde ETSI TS 119 312 |
| **2. Extensions** | | | | |
| **2.1. Authority Key Identifier** | Identificador de la clave del Issuer | No | NO | OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es Obligatorio siempre y cuando la clave pública de la AC se distribuya en formato de certificado "AUTOFIRMADO" |
| 2.1.1. KeyIdentifier | | No | | Derivado de la clave pública |
| **2.2. Subject Key Identifier** | Identificador de la clave del Subject | SI | NO | OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2) |
| 2.2.1. KeyIdentifier | | SI | | Derivado de la clave pública |
| **2.3. Key Usage** | | SI | SI | OID 2.5.29.15 |
| 2.3.1. Digital Signature | Seleccionado “1” | SI | | |
| 2.3.2. Content commintment | Seleccionado “1” | SI | | |

| | | | | |
|---|---|---|---|---|
| 2.3.3. Key Encipherment | Seleccionado “1” | SI | | |
| 2.3.4. Data Encipherment | No seleccionado. “0” | | | |
| 2.3.5. Key Agreement | No seleccionado. “0” | | | |
| 2.3.6. Key Certificate Signature | No seleccionado. “0” | | | |
| 2.3.7. CRL Signature | No seleccionado. “0” | | | |
| 2.3.8. Encipher Only | No seleccionado. “0” | | | |
| 2.3.9. Decipher Only | No seleccionado. “0” | | | |
| **2.4. Certificate Policies** | | SI | NO | OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2) |
| 2.4.1. Policy Information | | SI | | |
| 2.4.1.1. Policy Identifier | 1.3.6.1.4.1.oid_AC.2.3.2 | SI | | Identificador de la política de la AC |
| 2.4.1.2. Policy Qualifiers | | SI | | |
| 2.4.1.1.1 CPS URI | (https://www.repo_example.com/dpc/) | SI | | OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada |
| 2.4.1.1.2. User Notice/Explicit text | “CERTIFICADO DE REPRESENTANTE LEGAL EN DISPOSITIVO SEGURO DE CREACION DE FIRMA - DSCF" | SI | | OID 1.3.6.1.5.5.7.2.2 Texto indicativo |
| **2.5. Subject Alternative Names** | | NO | NO | OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2) |
| 2.5.1. rfc822Name | Correo electrónico del Signatario "nombreapellido@example.com.ec" | SI | | |
| **2.6. Extended Key Usage** | | SI | NO | OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2) |
| 2.6.1. clientAuth | Presente (1.3.6.1.5.5.7.3.2) | SI | | Transport Layer Security (TLS) World Wide Web (WWW) client authentication |
| 2.6.2. Email protection | Presente (1.3.6.1.5.5.7.3.4) | NO | | Sólo se activa si se incluye el correo electrónico del Signatario |
| **2.7. cRLDistributionPoint** | | SI | NO | OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2) |
| 2.7.1. distributionPoint | (http://crl1.example.com/example1subordinada.crl) | SI | | http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETFRFC 4516 [4] scheme |
| 2.7.2. distributionPoint | (http://crl2.example.com/example2subordinada.crl) | No | | http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETFRFC 4516 [4] scheme |
| **2.8. Authority Information Access** | | SI | NO | OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2) |
| 2.8.1. Access Description | | SI | | |
| 2.8.1.1. Access Method | id-ad-ocsp | Si | | OID 1.3.6.1.5.5.7.48.1 |
| 2.8.1.1.1 Access Location | (http://ocsp1.example.com/ocsp/) | Si | | URL de acceso al OCSP(http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5] |
| 2.8.1.1.2. Access Location | (http://ocsp2.example.com/ocsp/) | No | | URL de acceso al OCSP (http://) IETF RFC 7230-7235 |

| | | | | |
|---|---|---|---|---|
| | | | | [3] or https (https:// IETF RFC 2818 [5] |
| 2.8.2. Access Description | | No | | No es Obligatorio siempre y cuando incluya la ubicación de acceso al OCSP |
| **2.9. Basic Constraints** | | SI | SI | OID 2.5.29.19 |
| 2.9.1. cA | FALSE | SI | | |

### 7.1.1. Número de Versión.

El número de versión se encuentra especificado dentro de cada perfil de certificado.

### 7.1.2. Extensiones del Certificado.

La extensión del certificado se encuentra especificado dentro de cada perfil.

### 7.1.3. Identificadores de Objetos de Algoritmos.

Los OID se encuentran especificados dentro de cada perfil de certificado.

### 7.1.4. Formas de los nombres.

Las formas de los nombres encuentran especificadas dentro de cada perfil de certificado.

### 7.1.5. Restricciones de Nombre.

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

### 7.1.6. Identificador de objeto de Política de Certificado.

El OID de los certificados es:

- OID de Representante Legal archivo: 1.3.6.1.4.1.37746.2.3.1
- OID de Representante Legal DSCF: 1.3.6.1.4.1.37746.2.3.2
- OID de Sello Electrónico en archivo: 1.3.6.1.4.1.37746.2.4.1
- OID de Sello Electrónico en DSCF: 1.3.6.1.4.1.37746.2.4.2
- OID de Sello de Tiempo: 1.3.6.1.4.1.37746.2.5.1

### 7.1.7. Uso de la extensión Restricciones de Política.

No es aplicable.

### 7.1.8. Sintaxis y Semántica de los calificadores de Política.

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.

**Tabla 1:** 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.repoexample.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 de la 5280 " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Las CRL's son firmadas por la autoridad de certificación que ha emitido los certificados.

### 7.2.1. Número de Versión.

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

### 7.2.2. CRL y extensiones de entrada CRL.

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

### 7.2.3. PERFIL OCSP.

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

Elementos característicos del perfil:

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

### 7.2.4. Número de Versión.

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

### 7.2.5. Extensiones OCSP.

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

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

- Incluye el OID de política aplicable al certificado OCSP: 1.3.6.1.4.1.37746.2.6.1
- Además, se publica la referencia documental de política:
  - DPC: https://www.securitydata.net.ec/normativas/dpcocsp.pdf
  - User Notice: "CERTIFICADO DE VALIDACION OCSP"

- Subject Alternative Name con OID 2.5.29.17 – NO CRÍTICA
  - Incluye rfc822Name con correo de contacto del servicio.

- CRL Distribution Points con OID 2.5.29.31 – NO CRÍTICA
  - Publica puntos de distribución de CRL del emisor.

- Authority Information Access con OID 1.3.6.1.5.5.7.1.1 – NO CRÍTICA
  - Publica caIssuers para descarga del certificado emisor (URL HTTP del emisor).

- Subject Key Identifier con OID 2.5.29.14 – NO CRÍTICA
  - Identificador de clave del sujeto para facilitar construcción y validación de cadena.

- Authority Key Identifier con OID 2.5.29.35 – NO CRÍTICA
  - Identificador de clave de la CA emisora para facilitar construcción y validación de cadena.

### 7.3. PERFIL CRL.

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

### 7.4. PERFIL OCSP.

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

## 8. Auditorías de Cumplimiento y Otros Controles.

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

### 8.1. FRECUENCIA 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. CALIFICACIONES DEL EVALUADOR.

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

## 8.3. RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA.

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

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. ASPECTOS CUBIERTOS POR LOS CONTROLES.

La auditoría verifica los siguientes principios:

a) Publicación de la Información: Que la AC hace públicas las Prácticas de Negocio y de Gestión de Certificados (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.

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

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

## 8.6. COMUNICACIÓN DE RESULTADOS.

El proceso de comunicación se encuentra definido en la DPC de Security Data.

# 9. Otras Cuestiones Legales y de Actividad.

## 9.1. TARIFAS.

### 9.1.1. Tarifas de Emisión de Certificado o Renovación.

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

### 9.1.2. Tarifas de Acceso 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.

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

### 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. Reembolsos.

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.

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

### 9.2.2. Otros Bienes.

Sin estipulación.

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

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

## 9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN.

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.

### 9.3.1. Ámbito de la Información Confidencial.

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

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

### 9.3.2. Información no Confidencial.

La AC mantendrá como información no privada la siguiente:

- La contenida en la presente 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.

### 9.3.3. Responsabilidad en la Protección de Información Confidencial.

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

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

## 9.4. PRIVACIDAD DE LA INFORMACIÓN PERSONAL.

### 9.4.1. Política de Privacidad.

Security Data tiene como política de privacidad lo establecido en el derecho de habeas data: “La información privada, será aquella que por versar sobre información personal o no, y que por encontrase 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 (LOPDP). 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.

### 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 Calificada como Privada.

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

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

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

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

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

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

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

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

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

### 9.4.7. Otras circunstancias de revelación de información.

No se estipula

## 9.5. DERECHOS DE PROPIEDAD INTELECTUAL.

SECURITY DATA, tiene derechos de propiedad intelectual sobre todos sus documentos normativos, planes, procesos, patentes, marca comercial, material comercial y certificados que 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.

Las declaraciones y garantías de la CA se encuentran estipuladas en la DPC.

### 9.6.2. Declaraciones y Garantías de la RA.

Las declaraciones y garantías de la RA se encuentran estipuladas en la DPC.

### 9.6.3. Declaraciones y Garantías de los Suscriptores.

Las declaraciones y garantías de los suscriptores se encuentran estipuladas en la DPC.

### 9.6.4. Declaraciones y Garantías de la parte que Confía.

Las declaraciones y garantías de la parte que confía se encuentran estipuladas en la DPC.

### 9.6.5. Declaraciones y Garantías de Otros Participantes.

Sin estipulación.

## 9.7. RENUNCIAS A GARANTÍAS.

SECURITY DATA por la presente renuncia a todas las garantías, incluida la garantía de comerciabilidad y / o idoneidad para un propósito particular que no sea en la medida prohibida por la ley o expresamente estipulada en esta 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 PC y su correspondiente DPC, o por cualquier otra responsabilidad en la que puedan incurrir en un contrato, agravio u otro, incluida la responsabilidad por negligencia por suscriptor o tercero de confianza o tercero por certificado, siempre que el suscriptor, el tercero de confianza o el tercero cumplan plenamente con lo establecido en la presente PC y DPC.

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

## 9.9. INDEMNIZACIONES.

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

## 9.10. PLAZO Y TERMINACIÓN.

### 9.10.1. Plazo.

Este documento de Política de Certificación y cualquier enmienda a este, entrarán en vigencia

tras su publicación en la web de SECURITY DATA y permanecerán vigentes hasta que sea reemplazado por una versión más nueva.

### 9.10.2. Terminación.

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

## 9.11. AVISOS Y COMUNICACIONES INDIVIDUALES CON LOS PARTICIPANTES.

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

Según lo definido en la DPC de Security Data.

## 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 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 Política 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 Política de Certificación y su DPC, 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.

| | | |
|---|---|---|
| **ELABORADO POR** | COORDINADOR DEL SISTEMA DE GESTIÓN | Solanch Andrea Castillo Rueda<br>Time Stamping Security Data |
| **REVISADO POR** | CHIEF TECHNOLOGY OFFICER (CTO) | Lenin Alberto Vasquez Gonzalez<br>Time Stamping Security Data |
| | SUPERVISOR LEGAL | Diego Eduardo Cevallos Nuquez<br>Time Stamping Security Data |

| SECURITYDATA TU IDENTIDAD DIGITAL, EN UNA FIRMA. | POLÍTICAS DE CERTIFICACIÓN REPRESENTANTE LEGAL | CÓDIGO | SD-ID-PE-16 |
|---|---|---|---|
| | | VERSIÓN | V10 |
| | | FECHA DE APROBACIÓN | 25/02/2026 |
| | | PÁGINAS | 69 |

| APROBADO POR | GERENTE GENERAL | Firmado electrónicamente por: CESAR NAPOLEON SANTANA VILLAMAR |
|---|---|---|