SECURITY DATA
TU IDENTIDAD DIGITAL, EN UNA FIRMA.

POLÍTICA DE CERTIFICACIÓN DE SELLO ELECTRÓNICO

diciembre 22

2025

Contenido

1. Introducción.

1.1. PRESENTACIÓN.

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

Security Data Seguridad en Datos y Firma Digital S.A. (en adelante Security Data), es una empresa constituida de acuerdo a la legislación ecuatoriana, inscrita en el registro mercantil bajo el numero 2246 el 13 de Julio del 2010 con existencia legal hasta el 13 de Julio del 2060.

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

1.2. NOMBRE DE DOCUMENTO.

1.2.1. Frecuencia de revisión.

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

1.2.2. Procedimiento de aprobación.

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

1.2.3. Persona de Contacto.

Persona contacto:	Lenin Alberto Vásquez Gonzalez
Correo electrónico:	lenin.vasquez@securitydata.net.ec
Dirección:	Alonso de Torres y Av. Del Parque oficinas administrativas C8
Número de teléfono:	023922169 Ext. 5001
Sitio Web:	www.securitydata.net.ec
Identificador:	OID de archivo: 1.3.6.1.4.1.37746.2.4.1 OID de DSCF: 1.3.6.1.4.1.37746.2.4.2

2. Descripción General.

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

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

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

2.1. DESCRIPCIÓN DE LOS CERTIFICADOS.

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

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

Estos certificados pueden ser emitidos en los siguientes soportes:

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

3. Marco Normativo y referencias.

Esta Política se rige por lo dispuesto en:

- Normativa Técnica de ARCOTEL aplicable a servicios de certificación y sellado de tiempo.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- ETSI EN 319 421 – Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

4. Participantes en los Servicios de Certificación.

4.1. AUTORIDAD DE CERTIFICACIÓN.

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

4.2. PRESTADOR DE SERVICIOS DE CERTIFICACIÓN.

El Prestador de Servicios Electrónicos de Certificación (PSC) es la persona, física o jurídica, que presta uno o más servicios de certificación. Security Data es un PSC en cumplimiento con su Declaración de Prácticas de Certificación (DPC) que emite certificados reconocidos según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

4.3. SUSCRIPTORES.

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

4.4. TERCEROS QUE CONFÍAN.

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

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

4.5. CERTIFICADO DE SELLO ELECTRÓNICO.

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

5. Uso de los Certificados.

5.1. USO PERMITIDO DEL CERTIFICADO.

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

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

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

5.2. USOS NO AUTORIZADOS DE LOS CERTIFICADOS.

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

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

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

6. Definiciones y Acrónimos

6.1. DEFINICIONES.

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

Clave Pública y Clave Privada: La criptografía asimétrica en la que se basa la PKI emplea un par de claves (podrían ser dos pares de claves), lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

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

Sello electrónico: Conjunto de datos en formato electrónico, creado mediante medios criptográficos seguros y asociado a un certificado de sello electrónico, que permite identificar a la entidad emisora y garantizar la integridad y autenticidad de los datos electrónicos a los que se aplica.
Función Hash: Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

Listas de Certificados Revocados (CRL): lista donde figuran las relaciones de certificados revocados o suspendidos.

Módulo Criptográfico Hardware (HSM): Módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

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

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

6.2. ACRÓNIMOS.

AC:	Autoridad de Certificación
AC Sub:	Autoridad de Certificación Subordinada
PC:	Política de Certificación
DPC:	Declaración de Prácticas de Certificación
CRL:	Lista de Certificados Revocados (Certificate Revocation List)
HSM:	Módulo de seguridad criptográfico (Hardware Security Module)
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
PKI:	Infraestructura de Clave Pública (Public Key Infrastructure)
PSC:	Prestador de Servicios de Certificación
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:	Único de Transformation Format – 8 bits.

7. Identificación y Autenticación.

7.1. REGISTRO DE NOMBRES.

7.1.1. Tipos de Nombres.

Todos los certificados requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500. Adicionalmente, todos los nombres de los certificados reconocidos son coherentes con lo dispuesto en las normas:

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

7.1.2. Necesidad de que los nombres sean significativos.

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

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

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

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

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

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

7.1.4. Seudónimos.

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

7.1.5. Singularidad de los Nombres.

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

8. Validación Inicial de Identidad.

8.1. MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA.

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.

8.2. AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA).

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

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

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

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

8.3. AUTENTICACIÓN DE LA IDENTIDAD EN LA RENOVACIÓN DE CERTIFICADOS.

En el supuesto de renovación de la clave, Security Data informará previamente al suscriptor sobre los cambios que se hayan producido en los términos y condiciones respecto a la emisión anterior.

Se podrá emitir un nuevo certificado manteniendo la anterior clave pública, siempre que siga considerándose criptográficamente segura.

8.4. IDENTIFICACIÓN Y AUTENTICACIÓN EN LA REVOCACIÓN DE CERTIFICADOS.

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 Tercero Vinculado de Security Data Seguridad en Datos y Firma Digital: deberá identificar al suscriptor ante una petición de revocación según los propios medios que considere necesarios.

8.5. INFORMACIÓN DE TITULAR NO VERIFICADA.

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

9. Responsabilidades y Obligaciones.

9.1. OBLIGACIONES DE LOS SUSCRIPTORES.

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

- Cumplir en todo momento con las normas y regulaciones emitidas por Security Data en su DPC y las correspondientes Políticas de Certificados.

- Comunicar a Security Data cualquier modificación o variación de los datos que se aportaron para obtener el Certificado de Sello Electrónico.
- Verificar, a través de la Lista de Certificados Revocados, el estado de los Certificados de sello electrónico.
- Proteger y conservar el Dispositivo Seguro de Creación de Firma.\o a su vez el acceso al certificado en software.
- La revocación del certificado y la emisión de uno nuevo a Security Data en caso de olvido de la clave de protección del Certificado de Sello Electrónico.
- Responder por el uso del Certificado de Sello Electrónico y de las consecuencias que se deriven de su utilización.
- Cumplir con lo estipulado en el artículo 17 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Respetar lo dispuesto en los instrumentos jurídicos vinculantes con la AC.
- El Suscriptor será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta PC.

9.2. OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN.

Las responsabilidades de los terceros que confían son las siguientes:

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

9.3. OBLIGACIONES DE SECURITY DATA.

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

Security Data presta los servicios de Certificación Digital conforme con esta Política de certificación, Declaración de Prácticas de Certificación y a los estándares de aplicación. Además de:

- Emitir Certificados conforme a esta PC y a lo establecido en la DPC y a los estándares de aplicación.
- Emitir Certificados cuyo contenido mínimo sea definido en la PC y DPC vigentes.
- Emitir Certificados según la información que obra en su poder y libres de errores de entrada de datos.

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

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

10.1. SOLICITUD DE CERTIFICADOS.

10.1.1. Quién puede solicitar un Certificado.

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

10.1.2. Procesos de Solicitud de Certificados.

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

10.2. VALIDEZ DEL CERTIFICADO DE SELLO ELECTRÓNICO.

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

10.3. PROCEDIMIENTO DE TRAMITACIÓN.

10.3.1. Autenticación de Identidad.

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

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

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

10.3.2. Aprobación o rechazo de la solicitud de certificados.

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

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

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

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

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

10.3.3. Aprobación o rechazo de la solicitud de certificados.

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

10.4. EMISIÓN DEL CERTIFICIADO.

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

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

Según lo definido en la DPC de Security Data.

10.4.2. Entrega del Certificado.

Según lo definido en la DPC de Security Data.

10.5. ACEPTACIÓN DEL CERTIFICADO.

Según lo definido en la DPC de Security Data.

10.5.1. Devolución.

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 email firmado electrónicamente 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.

10.5.2. Publicación del Certificado.

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

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

No se efectúa notificación a terceros.

10.6. RENOVACIÓN DE CERTIFICADOS.

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

10.6.1. Personas autorizadas para solicitar renovación.

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

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

10.6.2. Aprobación o rechazo de las solicitudes de renovación.

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

10.6.3. Notificación de la Renovación del Certificado.

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

10.6.4. Aceptación de la Renovación del Certificado.

Según lo definido en la DPC de Security Data.

10.6.5. Publicación del Certificado Renovado.

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

10.7. MODIFICACIÓN DE CERTIFICADOS.

No es aplicable.

10.8. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.

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

10.9. 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.

11. Controles de Seguridad Física, Instalaciones, Gestión y Operacionales.

Security Data implementará medidas técnicas y organizativas que garanticen:

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

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

a) Control y Detección de Incidentes.

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

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

b) Registro de Incidentes.

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

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

11.1. CONTROLES DE SEGURIDAD FÍSICA.

Según lo definido en la DPC de Security Data.

11.2. CONTROLES DE PROCEDIMIENTO.

Según lo definido en la DPC de Security Data.

11.3. CONTROLES DE PERSONAL.

Según lo definido en la DPC de Security Data.

11.4. CONTROLES DE SEGURIDAD TÉCNICA.

Según lo definido en la DPC de Security Data.

12. Perfiles de Certificados.

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

a) Sello electrónico en archivo:

Campo	en Archivo	Oblig.	Crit.	Observaciones
De SELLO ELECTRÓNICO	Autenticación y Firma			OID 1.3.6.1.4.1.oid_AC.2.4.1
1. Basic 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. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	SI		OID 2.5.4.7
1.4.3. Organization Name(O)	Nombre de la AC Subordinada "Organización"	SI		OID 2.5.4.10
1.4.5. Common Name (CN)	Nombre de la AC Subordinada	SI		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity		SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Country Name (C)	País donde se encuentra registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	SI		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) Titular de la Firma (Ciudad) ej. QUITO	SI		OID 2.5.4.7
1.6.3. Organization Name (O)	Nombre de la Persona Jurídica (Pública o Privada) Titular de la Firma. Ej. CORPORACION FAVORITA	SI		OID 2.5.4.10

1.6.4. Organization Unit Name (OU)	Se especifica el Departamento o Área al que pertenece el Signatario	No		OID 2.5.4.11
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) Titular de la Firma a la que está vinculado el Sello Electrónico"VAT(CÓDIGO_PAIS)-RUC Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.6. Serial Number	Número de Registro Único de Contribuyente de la Persona Jurídica (Pública o Privada) Ej. "1716151413001"	SI		OID 2.5.4.5
1.6.7. Common Name (CN)	Descripción del uso que se le dará al Sello Electrónico. Ej. RECEPCION DE DOCUMENTOS EN VENTANILLA UNICA	SI		OID 2.5.4.3
1.6.8. Surname	Apellidos del Signatario que estará vinculado al sello (como consta en el documento oficial)	SI		OID 2.5.4.4
1.6.9. Given Name	Nombres del Signatario que estará vinculado al sello (como consta en el documento oficial)	SI		OID 2.5.4.42
1.7. Subject Public Key Info		SI		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública del Signatario	SI		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es Obligatorio siempre y cuando la clave pública de la AC se distribuya en formato de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado “1”	SI		
2.3.2. Content 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.102.2.4.1	SI		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		SI		
2.4.1.1.1 CPS URI	(https://www.repo_example.com/dpc/)	SI		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE SELLO ELECTRONICO EN ARCHIVO"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico) "info@example.com.ec"	SI		
2.6. Extended Key Usage		SI	NO	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	SI		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	NO		Sólo se activa si se incluye el correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico)
2.7. cRLDistributionPoint		SI	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	(http://crl1.example.com/example1subordinada.crl)	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) 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
2.8.2.1. Access Method	id-ad-calssuers	no		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	(http://www.example.com/subordinate1.crt)	No		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		SI	SI	OID 2.5.29.19

2.9.1. cA	FALSE	SI		

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

Campo	en Dispositivo Seguro de Creación de Firma DSCF	Oblig.	Crit.	Observaciones
De SELLO ELECTRÓNICO	Autenticación y Firma			OID 1.3.6.1.4.1.oid_AC.2.4.2
1. Basic 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. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	SI		OID 2.5.4.7
1.4.3. Organization Name(O)	Nombre de la AC Subordinada "Organización"	SI		OID 2.5.4.10
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAIS)-IDENTIFICAR_ORGANIZACIÓN" Ej. VATEC-1716151413001	NO		2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	Nombre de la AC Subordinada	SI		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity		SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Country Name (C)	País donde se encuentra registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	SI		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) Titular de la Firma (Ciudad) ej. QUITO	SI		OID 2.5.4.7
1.6.3. Organization Name (O)	Nombre de la Persona Jurídica (Pública o Privada) Titular de la Firma. Ej. CORPORACION FAVORITA	SI		OID 2.5.4.10
1.6.4. Organization Unit Name (OU)	Se especifica el Departamento o Área al que pertenece el Signatario	No		OID 2.5.4.11
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) Titular de la Firma a la que está vinculado el Sello Electrónico"VAT(CÓDIGO_PAIS)-RUC Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.6. Serial Number	Número de Registro Único de Contribuyente de la Persona Jurídica (Pública o Privada) Ej. "1716151413001"	SI		OID 2.5.4.5

1.6.7. Common Name (CN)	Descripción del uso que se le dará al Sello Electrónico. Ej. RECEPCION DE DOCUMENTOS EN VENTANILLA UNICA	SI		OID 2.5.4.3
1.6.8. Surname	Apellidos del Signatario que estará vinculado al sello (como consta en el documento oficial)	SI		OID 2.5.4.4
1.6.9. Given Name	Nombres del Signatario que estará vinculado al sello (como consta en el documento oficial)	SI		OID 2.5.4.42
1.7. Subject Public Key Info		SI		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública del Signatario	SI		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es Obligatorio siempre y cuando la clave pública de la AC se distribuya en formato de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado “1”	SI		
2.3.2. Content 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.102.2.4.2	SI		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		SI		
2.4.1.1.1 CPS URI	(https://www.repo_example.com/dpc/)	SI		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	“CERTIFICADO DE SELLO ELECTRONICO EN DISPOSITIVO SEGURO DE CREACION DE FIRMA - DSCF"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo

2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico) "info@example.com.ec"	SI		
2.6. Extended Key Usage		SI	NO	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	SI		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	NO		Sólo se activa si se incluye el correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico)
2.7. cRLDistributionPoint		SI	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	(http://crl1.example.com/example1subordinada.crl)	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) 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
2.8.2.1. Access Method	id-ad-caIssuers	SI		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	(http://www.example.com/subordinate1.crt)	No		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		SI	SI	OID 2.5.29.19
2.9.1. cA	FALSE	SI		

13. Disponibilidad del Servicio.

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

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

- Uso de sistemas de alimentación ininterrumpida.

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

14. Gestión del Ciclo de vida del módulo criptográfico.

Las prácticas de gestión del ciclo de vida del HSM se describen en la DPC de Security Data.

El hardware criptográfico utilizado es inspeccionado por personal de confianza (en presencia de al menos dos personas) en el control de transporte y almacenamiento, según lo definido en los procedimientos internos de Security Data.

14.1. CONTROL MULTIPERSONA (K DE N) DE LA CLAVE PRIVADA.

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

14.2. CUSTODIA DE LA CLAVE PRIVADA.

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

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

14.3. ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN EL MÓDULO CRIPTOGRÁFICO.

La clave privada de la AC raíz está custodiada por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multipersona, que consiste en que el acceso a las claves privadas de las AC requiere el concurso simultáneo de tres ACs, protegidos por una clave de acceso. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

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

14.4. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA.

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

14.5. MÉTODO PARA DESTRUIR LA CLAVE PRIVADA.

El método de destrucción se debe regir de acuerdo con lo definido en el Procedimiento para Archivamiento, Acceso y Destrucción a claves privadas archivadas del AC.

Criterios para la destrucción:

- En caso de manipulación no autorizada del dispositivo criptográfico.
- Cuando el dispositivo es reemplazado, se eliminan las claves de la AC del dispositivo.
- Por un funcionamiento incorrecto del software y hardware del dispositivo criptográfico.
- Respaldo y recuperación de la información del dispositivo criptográfico.
- En caso de que las claves contenidas en el dispositivo no sirvan para un propósito comercial válido.
- Levantamiento de un nuevo dispositivo criptográfico para su uso.

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

Los suscriptores pueden destruir sus claves privadas cuando se revoca o vence el certificado correspondiente si la clave privada ya no es necesaria. Esto debe hacerse de manera segura para garantizar que no haya pérdida, robo, compromiso o divulgación o uso no autorizado.

14.6. AUTORIDAD DE CERTIFICACIÓN RAÍZ.

Security Data opera con una infraestructura de clave pública propia, que consiste en una "Autoridad de Certificación Raíz" y servicio de respuesta OCSP.

La CA Raíz opera sin conexión (fuera de línea); todos los aspectos relacionados con la seguridad física y técnica están detallados en la Declaración de Prácticas de Certificación de Security Data y, publicada en repositorios públicos y de libre acceso en: www.securitydata.net.ec

15. Procedimientos de Auditoría de Seguridad.

15.1. TIPOS DE EVENTOS REGISTRADOS.

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

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

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

- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal que realiza tareas de confianza en la AC.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de suscriptor, si se gestiona esa información.
- Posesión de datos de activación, para operaciones con la clave privada de las AC.

15.2. FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA.

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

15.3. PERIODO DE CONSERVACIÓN DE LOS REGISTROS DE AUDITORÍA.

Se almacenará la información de los logs de auditoría el tiempo que se considere necesario para garantizar las seguridades del sistema en función de la importancia de cada log en concreto.

15.4. PROTECCIÓN DE LOS REGISTROS.

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

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

Los dispositivos son manejados en todo momento por personal autorizado.

15.5. PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA.

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

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

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

15.6. SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA.

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

16. 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.

16.1. FRECUENCIA DE LAS AUDITORIAS.

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

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

16.2. CUALIFICACIÓN DEL AUDITOR.

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.

16.3. Relación entre el Auditor y la Autoridad Auditada.

Las empresas que realizan las auditorías externas nunca representan ningún conflicto de intereses que pueda desvirtuar su actuación en su relación con SECURITY DATA.

No obstante, SECURITY DATA realizará auditorías internas planificadas con informes mensuales a la AC de la jerarquía para garantizar en todo momento su adecuación a los requerimientos marcados por las políticas de certificación de la jerarquía.

16.4. ASPECTOS CUBIERTOS POR LOS CONTROLES.

La auditoría verifica los siguientes principios:

a) Publicación de la Información: Que la AC hace públicas las Prácticas de Negocio y de Gestión de Certificados en la DPC, así como la política de privacidad de la información y protección de datos personales y proporciona sus servicios en conformidad condichas 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 delas 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.

17. Representaciones y Garantías.

SECURITY DATA representa, en la medida especificada en su PC y DPC, cumple, en todos los aspectos materiales, con la Pc y DPC, y todas las leyes y regulaciones aplicables.

SECURITY DATA garantiza que:

- Ha tomado medidas razonables para verificar que la información contenida en cualquier Certificado sea precisa en el momento de la emisión y se verifique de acuerdo con este documento.
- Los certificados se revocarán si Security Data cree o se le notifica que el contenido del certificado ya no es exacto, o que la clave asociada con un certificado se ha visto comprometida de alguna manera.
- Lleva a cabo el proceso de emisión de conformidad con este documento.
- La información proporcionada no contiene ninguna información falsa o engañosa.
- Todos los certificados solicitados cumplen con todos los requisitos materiales de este documento.

SECURITY DATA no ofrece otras garantías, y todas las garantías, expresas o implícitas, legales o de otro tipo, están excluidas en la mayor medida permitida por la ley aplicable, incluidas, entre otras, todas las garantías en cuanto a comerciabilidad o idoneidad para un propósito particular.

18. Excepciones de las Garantías.

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

19. Cese de Operaciones de la AC.

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

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

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

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

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

20. Conformidad con la ley aplicable.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento; Ley Orgánica de Defensa del consumidor, Ley Orgánica de Transparencia de la Información y Acreditación de ARCOTEL, Norma Técnica para la Prestación de Servicios de Certificación y Servicios Relacionados, emitida por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

21. Cumplimiento de la Ley Aplicable.

Los certificados emitidos por 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.

22. Control de Versiones.

Cesar Napoleon Santana Villamar
Time Stamping Security Data

VERSIÓN	CAMBIOS Y/O MODIFICACIONES	FECHA DE ACTUALIZACIÓN	ELABORADO POR	REVISADO POR	APROBADO POR
V1	EDICIÓN INICIAL	22/12/2025	SUPERVISOR LEGAL	CHIEF TECHNOLOGY OFFICER (CTO)	GERENTE GENERAL

Lenin Alberto Vasquez Gonzalez
Time Stamping Security Data