DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)

DE

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, S.A.

Versión 8.0

INDICE

1. MARCO LEGAL

1.1. Base Legal

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

1.2. Vigencia

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

1.3. Soporte Legal

1. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial No. 577 de 17 de abril de 2002.

2. De conformidad con lo dispuesto en el Art. 37 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el Consejo Nacional de Telecomunicaciones es el Organismo de autorización, registro y regulación de las Entidades de Certificación de Información y Servicios Relacionados Acreditados.

3. Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedido mediante Decreto Ejecutivo No. 3496 publicado en el Registro Oficial 735 de 31 de diciembre de 2002, y reformas constantes en Decreto Ejecutivo 1356 de 29 de septiembre de 2008, publicadas en el Registro Oficial No. 440 de 6 de octubre de 2008.

4. Que, el segundo artículo enumerado agregado por el artículo 4 del Decreto Ejecutivo No. 1356 a continuación del artículo 17 del Reglamento General a la Ley de Comercio EJectr6nico, Firmas Electrónicas y Mensajes de Datos, dispone que la acreditación como entidad de certificación de información y servicios relacionados, consistirá en un acto administrativo emitido por el CONATEL a través de una resolución que será inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados.

5. Resolución 477-20-CONATEL-2008 de 08 de octubre de 2008, se aprobó el modelo de resolución para la Acreditación como Entidad de Certificación de Información y Servicios Relacionados.

6. Resolución No. TEL-640-21-CONATEL-2010 de 22 de octubre de 2010, aprobó la petición de Acreditación de la Compañía SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. como Entidad de Certificación de Información y Servicios Relacionados, para los cual la SENATEL suscribió el respectivo acto administrativo, conforme el modelo aprobado por el Consejo Nacional de Telecomunicaciones.

1.4. Proceso de Resolución de Conflictos

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

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

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

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

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

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

La legislación aplicable es la ecuatoriana.

2. INTRODUCCIÓN

2.1. 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.

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

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

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

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

2.2. Nombre del Documento

2.2.1. Identificación

Nombre:	Declaración de Practicas de Certificación (DPC)
Versión:	8.0
Descripción:	Declaración de Practicas de Certificación de Security Data Seguridad en Datos y Firma Digital S.A.
Fecha de Emisión:	13 de Septiembre 2013

2.2.2. Publicación

Este documento puede obtenerse libremente en la dirección electrónica https://www.securitydata.net.ec

2.3. Definiciones y Acrónimos

2.3.1. 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.

2.3.2.Acrónimos

AC:	Autoridad de Certificación
AC Sub:	Autoridad de Certificación Subordinada
AR:	Autoridad de Registro
PC:	Política de Certificación
DPC:	Declaración de Prácticas de Certificación
CRL:	Lista de Certificados Revocados (Certificate Revocation List)
HSM:	Módulo de seguridad criptográfico (Hardware Security Module)
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.

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

2.4. Aspectos Generales

2.4.1. Obligaciones

2.4.1.1. Obligaciones de la AC

- Emitir Certificados conforme a este DPC y a las PCs correspondientes y a los estándares de aplicación.
- Emitir Certificados cuyo contenido mínimo sea definido en las Políticas de Certificados 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 las PCs de cada tipo de Certificado y, en su caso, de los contratos de prestación de servicios de certificación correspondientes y en el Acuerdo para la Autoridad de Registro.
- Facilitar el acceso a las versiones vigentes de la DPC y de las PCs de cada tipo de Certificados.

- Ofrecer y mantener la infraestructura necesaria para los servicios de certificación, así como los controles de seguridad física, de procedimientos y personales necesarios para la práctica de la actividad de certificación.
- 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.
- Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos.
- Colocar copias de sus propios certificados y de información de revocación a disposición de quien desee verificar una firma electrónica con referencia a dichos certificados, los cuales se publicarán en la página Web https://www.securitydata.net.ec
- Proporcionar la información mínima necesaria para el uso de los certificados al solicitante, cuya información deberá transmitirse de forma gratuita, por escrito o por vía electrónica.
- Tomar medidas contra la falsificación de certificados y garantizar la confidencialidad de los datos de creación de firma durante el proceso de generación, así como su entrega por un procedimiento seguro al suscriptor.
- No copiar ni almacenar los datos de creación de firma del suscriptor.
- Informar sobre las modificaciones de las Políticas de Certificados y de la Declaración de Prácticas de Certificación a los Suscriptores y Terceros vinculados.
- Cumplir con las obligaciones del presente DPC.
- Todas aquellas obligaciones impuestas por el presente DPC y en su caso, en la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos.
- Aprobar o negar las solicitudes de emisión de certificados digitales de firma electrónica, de acuerdo con lo establecido en esta DPC y en las PCs.
- Poner a disposición de los usuarios el listado de certificados revocados (CRL), la cual se publicará en la página Web https://www.securitydata.net.ec
- Custodiar por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo. A estos efectos, la SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL almacena en formato digital o en papel todas las versiones de la DPC publicadas y copia del contrato de prestación de servicios entre la Entidad de Certificación de Información y el suscriptor.
- Comunicar de manera inmediata a los titulares de los certificados emitidos por la ECI, el compromiso de su clave privada, pérdida, divulgación, modificación, uso no autorizado, con el fin de revocarlos.
- Efectuar la identificación y autenticación de los usuarios como pasos previos a la revocatoria de los certificados de firma electrónica.
- Proteger los datos personales de los solicitantes y usuarios de certificados digitales o electrónicos.
- Llevar a cabo cada uno de los pasos que se describan en el procedimiento de emisión de certificados de firma electrónica.

- Implementar y mantener los requerimientos de seguridad impuestos a la clave privada de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, de acuerdo a esta DPC y PCs.
- Ofrecer y mantener la infraestructura tecnológica necesaria para el establecimiento de una estructura, tanto en hardware como en software, para operar de acuerdo a los estándares internacionales.

2.4.1.2. Obligaciones del Tercero Vinculado

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

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

2.4.1.3. Obligaciones del Solicitante

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

2.4.1.4. Obligaciones del Suscriptor

- Cumplir en todo momento con las normas y regulaciones emitidas por la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL en su DPC y las correspondientes Políticas de Certificados.
- Comunicar a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL cualquier modificación o variación de los datos que se aportaron para obtener el Certificado de Firma Electrónica.
- Verificar, a través de la Lista de Certificados Revocados, el estado de los Certificados de firma electrónica.
- Proteger y conservar el Dispositivo Portable Seguro-Token.\o a su vez el acceso al certificado en software.
- Solicitar la revocación del certificado y la emisión de uno nuevo a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL en caso de olvido de la clave de protección del Certificado de Firma Electrónica.
- Responder por el uso del Certificado de Firma Electrónica y de las consecuencias que se deriven de su utilización.
- Cumplir con lo estipulado en el artículo 17 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

2.4.1.5. Obligaciones de los Usuarios

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

DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, políticas y procedimientos que se especifican en este DPC y en la PCs para cada tipo de certificado distinto.

2.4.2.Responsabilidades

2.4.2.1. Responsabilidad de la AC

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

2.4.2.2. Responsabilidad del Tercero Vinculado

- El Tercero Vinculado responderá de las funciones que le correspondan conforme a esta DPC y, en especial, asumirá toda la responsabilidad por la correcta identificación y

validación del Solicitante/Suscriptor, con las mismas limitaciones que se establecen en el apartado anterior con relación a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

- El Tercero Vinculado, responderá ante la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL por los daños y perjuicios que pudieran derivarse de la ejecución de esas funciones concertadas de manera negligente o en forma distinta a la contemplada en la presente DPC y en las PCs emitidas para cada tipo de certificado.
- No obstante, el Tercero Vinculado no se hace responsable, en ningún caso, de la identidad o identificación del solicitante y/o suscriptor en el supuesto de falsificación de la documentación u otros datos aportados, por él mismo o por el tercer que le suplante.

2.4.2.3. Responsabilidad del Suscriptor

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

2.4.2.4. Responsabilidad del Usuario

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

2.4.3.Entidades Participantes

2.4.3.1. Entidad Acreditada (EA)

Security Data Seguridad en Datos y Firma Digital es un Entidad Acreditada (EA) que emite certificados reconocidos según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Security Data Seguridad en Datos y Firma Digital es la entidad emisora de los certificados y responsable de las operaciones del ciclo de vida de los certificados. Las funciones de autorización, registro, emisión y revocación respecto de los certificados personales de entidad final, pueden ser realizadas por otras entidades por delegación soportada contractualmente con Security Data Seguridad en Datos y Firma Digital, que actuarán como intermediarios. Security Data Seguridad en Datos y Firma Digital también ofrece servicios de validación de firmas electrónicas y de sellado de tiempo, regidos por sus políticas particulares, no incluidas en este documento.

2.4.4.Autoridad de Certificación (AC)

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

2.4.4.1. 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.

2.4.4.2. Tercero Vinculado

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

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

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

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

- La propia Security Data Seguridad en Datos y Firma Digital directamente.

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

La entidad que actúe como Tercero Vinculado de Security Data Seguridad en Datos y Firma Digital 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 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 podrá delegar estas funciones a otra entidad o persona de confianza. Dicha entidad o persona deberá tener una especial vinculación con el Tercero Vinculado 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 en el que se acepte la delegación de estas funciones. Security Data Seguridad en Datos y Firma Digital deberá conocer y autorizar de manera expresa el acuerdo.

2.4.5. 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.

2.4.6. Suscriptor

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

2.4.7. 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.

2.4.8. Custodio de las Claves

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

2.4.9. Tercero que confía en los Certificados

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

Los certificados reconocidos emitidos por Security Data Seguridad en Datos y Firma Digital 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 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.

2.5. Tipos de Certificados

2.5.1. Certificados Corporativos Reconocidos

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

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

2.5.2. Certificados para la Administración Pública

Los certificados para la Administración Pública son certificados electrónicos emitidos según los requisitos establecidos en la Ley de Comercio electrónico, Firmas Electrónicas y Mensajes de Datos.

- Certificado de Funcionario Público: Son certificados reconocidos de persona natural que identifican al suscriptor como Administración Pública y al firmante como empleado de la Administración.

2.5.3. Certificados Privados

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

Certificados de Persona natural profesional: Son certificados reconocidos de persona natural profesional que identifican al suscriptor como una persona natural que tiene una profesión reconocida y debidamente sustentada y que pueden ser usados para este certificado para temas tributarios, legales y personales.

2.5.4. Certificados de Servidor Seguro

Certificados de Servidor Seguro: Son certificados que relacionan un dominio de Internet con una persona jurídica o un comerciante registrado determinado.

2.6. Tipos de Soporte

Los Certificados Corporativos, de Administración Pública o Privados pueden generarse en dos tipos de soporte hardware, software o roaming:

2.6.1. Dispositivo Seguro de Creación de Firma (DSCF)

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

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

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

Para activar el DSCF será necesario introducir el código de activación (PIN). Si se introduce el PIN seis veces seguidas de manera incorrecta, el dispositivo quedará bloqueado, y por lo tanto inservible. Para proceder al desbloqueo se deberá acercar al Tercero Vinculado donde adquirió el certificado con el dispositivo bloqueado o enviarlo a la misma, en donde se realizará el desbloqueo. El PIN es secreto y personal para el usuario, se le entregará un PIN inicial el que debe ser modificado posteriormente por el usuario utilizando las aplicaciones correspondientes.

2.6.2. Soporte en Software

2.6.2.1. Certificados, llaves Públicas y privadas en Software

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

2.6.2.2. Certificados, llaves públicas y privadas para servidor Web Seguro - SSL

Este servicio permite al usuario después de haber realizado la solicitud y siendo aprobada por la Entidad Certificadora, relacionar un dominio de Internet con una Persona Jurídica o un comerciante registrado y una vez haya recibido los códigos de generación, pueda acceder a al portal de Security Data y pueda generar el certificado digital, una vez que haya generado la solicitud en el Servidor web, permitiendo almacenarlo en el Servidor en un formato .CER.
Siendo el uso de estos certificados para la implementación de servidores Web Seguros.

2.6.2.3. Soporte en Roaming

Las claves privadas de los certificados emitidos en soporte Roaming se generan y almacenan de manera segura en el directorio LDAP propiedad de la CA. Este repositorio es seguro con doble capa de encriptación que permite almacenar las claves de manera segura. Las claves están protegidas por una contraseña, con esto se puede poner un doble factor de autenticación. Este soporte le da una solución flexible al no depender de dispositivos de hardware.

2.7. Uso particular de los certificados

2.7.1. Usos apropiados de los certificados

- El suscriptor podrá hacer uso del certificado de Firma Electrónica según lo establecido en esta política del certificado, en el contrato de prestación de servicios que suscriba con la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, y las DPC.
- 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 de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL con sus suscriptores, consecuencia de esto la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL podrá revocar el certificado y dar por terminado en contrato.
- Los usos autorizados de los Certificados emitidos por la ECI 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 esta PC, y en las DPCs.
- El Certificado de firma electrónica emitido por la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL al suscriptor, deberá ser utilizado tal y como son suministrados. Queda prohibido cualquier alteración del certificado por parte del usuario.
- Los certificados de firma electrónica no podrán ser utilizados para acciones ilícitas, de acuerdo a lo establecido en la legislación ecuatoriana.
- Los certificados de firma electrónica presentas 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.

2.8. 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 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.

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

2.9. Administración de las Políticas

2.9.1. Organización Responsable

El Departamento Técnico de Security Data Seguridad en Datos y Firma Digital es responsable de la administración de esta DPC y de las Políticas de Certificación.

2.9.2. Frecuencia de Revisión

La DPC y las distintas CP serán revisadas y si procede, actualizadas, anualmente.

2.9.3. Procedimiento de Aprobación

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

3. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

3.1. Repositorios

Los repositorios de Security Data Seguridad en Datos y Firma Digital están referenciados por la URL. 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.

3.2. Publicación de información

3.2.1. Políticas y Prácticas de Certificación

Tanto la DPC actual como las Políticas de Certificación de cada tipo de certificado estarán disponibles en formato electrónico en la Web de Security Data Seguridad en Datos y Firma Digital.

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.

3.2.2. Términos y Condiciones

La relación contractual entre Security Data Seguridad en Datos y Firma Digital y los Suscriptores está basada en la firma de un Contrato de Prestación de Servicios de Certificación y la aceptación de las Condiciones Generales de Contratación de Security Data Seguridad en Datos y Firma Digital publicadas en su web.

3.2.3. Difusión de los Certificados

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

3.3. Frecuencia de Publicación

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.

Security Data Seguridad en Datos y Firma Digital publicará de forma inmediata cualquier modificación en las políticas y prácticas de certificación.

3.4. Control de acceso a los repositorios

La DPC, las Políticas 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.

4. IDENTIFICACIÓN Y AUTENTICACIÓN

4.1. Registro de Nombres

4.1.1. 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 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile",
- RFC 3739 "Qualified Certificates Profile".

4.1.2. Necesidad de que los nombres sean significativos

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

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.

4.1.3. Reglas para interpretar varios formatos 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.

4.1.4. Unicidad de los nombres

El nombre distinguido (DN) de los certificados emitidos será único para cada suscriptor o firmante. El atributo de CIF o NIF se usan para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.

4.2. Validación Inicial de la Identidad

4.2.1. Método de Prueba de 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, el método de prueba de la posesión de la clave privada por el suscriptor será la entrega de PKCS#10 o una prueba criptográfica equivalente u otro método aprobado por Security Data Seguridad en Datos y Firma Digital.

4.2.2. Autenticación de la Identidad de una Persona Jurídica

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.

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.

4.2.3. Autenticación de la identidad de una persona natural

El Tercero Vinculado verificará de forma fehaciente la identidad de la persona natural identificada en el certificado. Para ello, la persona natural deberá personarse y presentar la Cedula de Identidad, pasaporte u otro medio reconocido en derecho que le identifique.

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

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

Si se trata de una persona natural profesional se verificará los datos de la profesión con la Entidad competente.

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.

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

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

- Security Data Seguridad en Datos y Firma Digital verificará la existencia de la entidad mediante sus propias fuentes de información.
- Un representante autorizado de la organización deberá firmar un contrato con Security Data Seguridad en Datos y Firma Digital, donde se especificarán los aspectos concretos de la delegación y las responsabilidades de cada agente.
- Además se exigirá al Tercero Vinculado el cumplimiento de lo siguiente respecto de los operadores del Tercero Vinculado:
    - Verificar y validar la identidad de los nuevos operadores del Tercero Vinculado. El Tercero Vinculado deberá enviar a Security Data Seguridad en Datos y Firma Digital la documentación correspondiente al nuevo operador, así como su autorización a que actúe como operador de Tercero Vinculado.
    - Asegurar que los operadores del Tercero Vinculado hayan recibido formación suficiente para el desempeño de sus funciones, asistiendo como mínimo a una sesión de formación de operador.
    - Asegurar que la comunicación entre el Tercero Vinculado y Security Data Seguridad en Datos y Firma Digital se realiza de forma segura mediante el uso de certificados digitales de operador.

4.2.5. Validación del Correo Electrónico

En general, los firmantes son personas vinculadas con la Autoridad de Registro (por ejemplo, bancos, organizaciones, etc.)

Uno de los códigos de generación del certificado de firma electrónica es enviado a la dirección de correo electrónico proporcionado por el solicitante, de esta manera quedaría validada dicha dirección.

4.3. Identificación y Autenticación en la Renovación de Certificados

El suscriptor se podrá identificar y autenticar en el proceso de renovación si se cumple lo siguiente:

- El Tercero Vinculado ha autorizado la renovación.
- El certificado que desea renovar no ha caducado (hasta un día antes de la fecha de expiración).
- El suscriptor cumple con los requisitos para renovar un certificado. Los documentos para renovación que se encuentran detallados en la "Política de Certificación" de cada tipo de certificado concreto.

4.4. 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.

5. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

5.1. Solicitud de Certificados

5.1.1. Quién puede solicitar un Certificado

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

5.1.2. Procesos de Solicitud de Certificados

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

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

En las políticas de certificación (CP) se especifica la documentación requerida para la solicitud de cada tipo de certificado.

5.2. Validez del Certificado de Firma Electrónica

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

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

5.3. Tramitación de las Solicitudes de Certificados

5.3.1. Realización de las funciones de identificación y autenticación

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

5.3.1.1. Validación presencial de la identidad y de la documentación

La validación de la identidad y de la documentación presentada se la hará en forma presencial ante un operador de Tercero Vinculado, el cual validará la identidad del solicitante por medio de los documentos de identificación y revisará la validez de los documentos solicitados. Una vez validada la identidad y los documentos se procederá con la entrega del token al suscriptor.

5.3.1.2. Validación de la identidad mediante video conferencia

La validación de la identidad podrá efectuarse mediante videoconferencia ante un operador 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 ante un operador del Tercero Vinculado. Una vez validada la identidad y los documentos se procederá con la entrega del token al suscriptor enviándolo de forma segura al lugar donde se encuentre el suscriptor.

5.3.2. Aprobación o denegación de las solicitudes de certificados

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

Si la información no es correcta, el Tercero Vinculado denegará la petición, contactando al solicitante para comunicarle el motivo.

Si es correcta, el solicitante recibirá un mail indicando que su solicitud ha sido aprobada y que debe acercarse a la Autoridad de Registro y personarse para la confirmación de los datos, 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.

5.4. Emisión de Certificados

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

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 acciones siguientes:

a) Para los certificados en soporte hardware:

- El Tercero Vinculado le hará entrega del token. En caso de que el solicitante aporte su propio dispositivo, éste deberá ser homologado por Security Data Seguridad en Datos y Firma Digital previamente a su utilización. los Terceros Vinculados dispondrán de una lista de dispositivos homologados
- Activación del dispositivo: En el caso que el solicitante no disponga de ellos, se generarán los datos de activación del dispositivo y de acceso a la clave privada que contendrá.
- Generación del par de claves: Se procederá a la generación de los códigos de generación en la AC.
- El Tercero Vinculado hará entrega de uno de los códigos de generación de forma escrita. El segundo código de generación se lo enviará al solicitante al correo electrónico que haya sido proporcionado en la solicitud.

b) Para los certificados en Software:

El solicitante recibirá por correo electrónico una de las claves para la emisión del certificado. La segunda clave le será entregada personalmente en el Tercero Vinculado conjuntamente con la factura. Estas claves deben ser ingresadas en la página web https://www.securitydata.net.ec siguiendo las instrucciones del Tercero Vinculado. Una vez hecho este ingreso se procede a la emisión del certificado que será bajado al computador del solicitante.

5.4.2. Entrega del certificado.

Cuando el Suscriptor tenga las dos claves generadas (Código de Autorización y Número de Referencia), podrá generar el certificado.

a) En Software

Las dos claves deben ser ingresadas en la página web https://www.securitydata.net.ec y deberá seguir el procedimiento que se describe en el Manual de Activación del Certificado vía Software. Una vez realizado el procedimiento se emite el certificado, el mismo que se instalará el solicitante en su computador.

b) En Hardware

Las dos claves deben ser ingresadas en la página web https://www.securitydata.net.ec y deberá seguir el procedimiento que se describe en el Manual de Activación del Certificado vía Hardware. Una vez realizado el procedimiento se emite el certificado, el mismo que se instalará el Dispositivo criptográfico.

5.5. Aceptación del Certificado

5.5.1. Forma en la que se Acepta el Certificado

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

Como evidencia de la aceptación deberá quedar una hoja de aceptación firmada por el solicitante. El certificado se considerará válido a partir de la fecha en que se firmó la hoja de aceptación.

La hoja de aceptación deberá ser entregada al Tercero Vinculado físicamente y esta deberá ser firmada digitalmente una vez que el suscriptor disponga de la correspondiente firma digital. El archivo físico procederá a ser destruido.

5.5.2. Publicación del Certificado

Una vez el certificado generado y aceptado por el suscriptor o firmante, el certificado podrá ser publicado en los repositorios de certificados que se consideren necesarios.

5.6. Usos de las Claves y el Certificado

5.6.1. Uso de la Clave Privada y del Certificado por el Suscriptor

Los certificados podrán ser utilizados según lo estipulado en esta DPC y en la Política de Certificación correspondiente. La extensión Key Usage podrá ser utilizada para establecer límites técnicos a los usos de la clave privada del certificado correspondiente. La aplicación de estos límites dependerá en gran parte de su correcta implementación por aplicaciones informáticas de terceros, quedando su regulación fuera del alcance de este documento.

5.6.2. Uso de la Clave Pública y del Certificado por los Terceros que confían en los Certificados

Los terceros que confían en los certificados podrán utilizar los certificados para aquello que establece la presente DPC y la Política de Certificación correspondiente.

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.

5.7. Renovación de Certificados sin Cambio de Claves

No se contempla esta opción.

5.8. Renovación con Cambio de Claves

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

.

5.9. Modificación de Certificados

En caso de necesidad de modificar algún dato, el Tercero Vinculado deberá proceder a la revocación y a la emisión de un nuevo certificado.

5.10. Revocación y Suspensión de Certificados

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.

5.10.1. Causas para la revocación

Un certificado podrá ser revocado debido a las siguientes causas:

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

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

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

- Compromiso de la clave privada o de la infraestructura o sistemas de la AC, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
- Infracción, por parte de la AC o del 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.

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

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

d) Circunstancias que afectan al suscriptor:

- Finalización de la relación jurídica entre la 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.

e) Otras circunstancias:

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

5.10.2. 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.
- 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 del Tercero Vinculado a la que pertenece el suscriptor del certificado.
- Los operadores autorizados de la AC.
- Los mismos usuarios accediendo a la administración de su certificado.

5.10.3. Procedimientos de Solicitud de Revocación

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

En todo caso, al tiempo de suspenderse o revocarse el certificado, se enviará un comunicado al suscriptor, comunicando la hora y la causa de la misma.

5.10.3.1. Procedimiento Online

Security Data Seguridad en Datos y Firma Digital pondrá a disposición del suscriptor un sistema de revocación en línea disponible las 24 horas al día, 7 días a la semana y 365 días del año, Para ello, el suscriptor deberá:

- Acceder a la web de Security Data Seguridad en Datos y Firma Digital en el apartado correspondiente a revocación.
- Ingresar a la Administración de Cuenta (Manager Account).
- Buscar el Certificado Digital por Nombre y Apellido o email.
- Ingresar la contraseña de ingreso al sistema de Revocación.
- Ingresar a la Opción de Revocación del Certificado
- Introducir la causa de revocación.

Una vez aceptado, el certificado será inmediatamente revocado.

5.10.3.2. Revocación en Horario de Oficina

El suscriptor o el firmante deberá ponerse en contacto con el Tercero Vinculado de Security Data Seguridad en Datos y Firma Digital ya sea personal- o telefónicamente.

Si se presenta personalmente la identidad del suscriptor o firmante quedará autenticada mediante su cédula de identidad o pasaporte y se podrá proceder a la revocación inmediata del certificado.

Si lo hace vía telefónica al 1800-firmas / 1800-347627, el certificado quedará suspendido hasta que el suscriptor o firmante se presenten personalmente ante el Tercero Vinculado o envíen una carta o fax pidiendo la revocación del certificado. El certificado quedará suspendido por un periodo máximo de 15 días al cabo de los cuales éste será revocado. Dentro de estos 15 días el solicitante o firmante puede cancelar la suspensión y el procedimiento de revocación.

Se enviará un mensaje al Tercero Vinculado y al cliente con los datos de suspensión y/o revocación y el motivo.

5.10.3.3. Revocación Fuera de Horario de Oficina

Ver 5.12.3.1 Procedimiento Online

5.10.4. Plazo en el que la AC debe Resolver la Solicitud de Revocación

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

5.10.5. Obligación de Verificación de las Revocaciones por los Terceros

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.

5.10.6. Frecuencia de Emisión de CRLs

La CRL de los certificados de entidad final se emiten al menos cada 24 horas, o cuando se produzca una revocación, con una validez de 7 días.

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

5.10.7. Tiempo Máximo entre la Generación y la Publicación de las CRL

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

5.10.8. Disponibilidad del Sistema en Línea de Verificación del Estado de los Certificados

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.

5.10.9. 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.

5.10.10. Circunstancias para la 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 Consejo Nacional de Telecomunicaciones, 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.

5.10.11. 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 accediendo a la administración de su certificado.

5.10.12. Límites del Periodo de Suspensión

El límite lo establece el cliente mismo o a su vez la validez del certificado.

5.11. Servicios de Información del Estado de Certificados

5.11.1. 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.

Adicionalmente, Security Data Seguridad en Datos y Firma Digital ofrece el servicio de validación de certificados mediante el protocolo OCSP (Online Certificate Status Protocol).

5.11.2. 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.

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 se encuentre disponible en un lapso no mayor de 24 horas.

5.11.3. Finalización de la Suscripción

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

6. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

6.1. Controles Físicos

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

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

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

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

6.1.1. Ubicación Física y Construcción

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

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

6.1.2. Acceso Físico

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

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables así como Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

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

6.1.3. Alimentación Eléctrica y Aire Acondicionado

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

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

6.1.4. Exposición al Agua

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

6.1.5. Protección y Prevención de Incendios

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

6.1.6. Sistema de Almacenamiento

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

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

6.1.7. Eliminación de los Soportes de Información

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

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

6.2. Controles de Procedimiento

6.2.1. Roles de los Responsables

Los roles de confianza son los que se describen en las respectivas Políticas de Certificación de la jerarquía de forma que se garantiza una segregación de funciones que disemina el control y limita el

fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación. Los roles mínimos establecidos son:

- **Responsable de seguridad (Security Officer):** Mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad
- **Administradores del sistema de certificación (System Administrators):** Autorizado para realizar cambios en la configuración del sistema, pero sin acceso a los datos del mismo.
- **Operadores de sistemas (System Operator):** Responsables de la gestión del día a día del sistema (Monitorización, backup, recovery,...)
- **Auditor interno (System Auditor):** Autorizado a acceder a los logs del sistema y verificar los procedimientos que se realizan sobre el mismo.
- **Operador de AC - Operador de Certificación:** Responsables de activar las claves de la AC en el entorno Online, o de los procesos de firma de certificados y CRL's en el entorno Root Offline.
- **Operador de Tercero Vinculado (Registration Officer):** Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final.

6.2.2.Número de Personas Requeridas por Tarea

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

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

6.2.3.Identificación y Autenticación por Rol

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

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

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

6.2.4.Roles que Requieren Segregación de Funciones

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

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

6.3. Controles de Personal

6.3.1. Requisitos Relativos a la Calificación, Conocimiento y Experiencia Profesionales

Todo el personal que realiza tareas calificadas como confiables sin supervisión, lleva al menos seis meses trabajando en el centro de producción y tiene contrato laboral fijo.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

La AC se asegura que el personal de registro es personal confiable de una Corporación para realizar las tareas de registro. A tal efecto se exige una declaración en tal sentido por parte de la Entidad que asume funciones del Tercero Vinculado.

El empleado del registro habrá realizado un curso de preparación para la realización de las tareas de registro y validación de las peticiones. Al final de dicho curso, un auditor externo procederá a evaluar sus conocimientos del proceso.

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

6.3.2. Procedimientos de Comprobación de Antecedentes

Security Data Seguridad en Datos y Firma Digital realiza las investigaciones pertinentes antes de la contratación de cualquier persona.

Los Terceros Vinculados pueden establecer criterios diferentes, siendo responsables por la actuación de las personas que autoricen.

6.3.3. Requerimientos de Formación

Security Data Seguridad en Datos y Firma Digital realiza los cursos necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada operador.

6.3.4. Requerimientos y Frecuencia de Actualización de la Formación

Se realizarán actualizaciones con una frecuencia anual, salvo por modificaciones a la DPC, que serán notificadas a medida que sean aprobadas.

6.3.5. Requisitos de Contratación de Terceros

Los empleados contratados para realizar tareas confiables deberán firmar anteriormente las cláusulas de confidencialidad y la requerimientos operacionales empleados por la AC. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

6.4. Procedimientos de Auditoría de Seguridad

6.4.1. Tipos de eventos registrados

Security Data Seguridad en Datos y Firma Digital 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 la AC a través de la red.
- Intentos de accesos no autorizados a la red interna de la AC.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la Autoridad de Certificación.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC 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 la AC.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

Adicionalmente, Security Data Seguridad en Datos y Firma Digital conserva, ya sea manual o electrónicamente, la siguiente información:

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

6.4.2.Frecuencia de Procesado de Registros de Auditoría

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

6.4.3.Periodo de Conservación de los Registros de Auditoría

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

6.4.4.Protección de los Registros de Auditoría

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

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

Los dispositivos son manejados en todo momento por personal autorizado.

6.4.5.Procedimientos de Respaldo de los Registros de Auditoría

Security Data Seguridad en Datos y Firma Digital dispone de un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

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

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

6.4.6.Sistema de Recogida de Información de Auditoría

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

6.4.7.Análisis de Vulnerabilidades

La AC realiza periódicamente una revisión de discrepancias en la información de los logs y actividades sospechosas, de acuerdo al procedimiento interno establecido al efecto en las políticas de seguridad.

6.5. Archivo de Registros

6.5.1. Tipo de Eventos Archivados

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

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

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

6.5.2. Periodo de Conservación de Registros

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservarán durante el periodo que establezca la legislación vigente cuando sea aplicable. Los certificados se conservarán publicados en el repositorio durante al menos un año desde su expiración. Los contratos con los suscriptores y cualquier información relativa a la identificación y autenticación del suscriptor serán conservados durante al menos 15 años o el periodo que establezca la legislación vigente.

6.5.3. Protección del Archivo

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

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

6.5.4. Procedimientos de Copia de Seguridad del Archivo

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

6.5.5. Requerimientos para el Sellado de Tiempo de los Registros

Los registros están fechados con una fuente fiable.

Existe dentro de la documentación técnica y de configuración de la AC un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

6.5.6. Sistema de Archivo de Información de Auditoría

No estipulado.

6.6. Procedimientos para Obtener y Verificar Información Archivada

Durante la auditoria requerida por esta DPC, el auditor verificará la integridad de la información archivada.

El acceso a la información archivada se realiza solo por personal autorizado.

La AC proporcionará la información y los medios al auditor para poder verificar la información archivada.

6.7. Cambio de Claves de la AC

6.7.1. AC Raíz

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

La documentación técnica y de seguridad de la AC detalla el proceso de cambio de claves de la AC.

6.7.2. AC Subordinada

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

6.8. Plan de Recuperación de Desastres

6.8.1. Procedimientos de Gestión de Incidentes y Vulnerabilidades

La AC ha desarrollado un plan de contingencias, detallado en el documento "Política de Seguridad", para recuperar todos los sistemas en menos de 48 horas, aunque se asegura la revocación y publicación de información del estado de los certificados en menos de 24 horas.

Cualquier fallo en la consecución de las metas marcadas por este plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

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

En el caso de que tuviera lugar un incidente que alterara o corrompiera tanto recursos de hardware, software como datos, Security Data Seguridad en Datos y Firma Digital procederá según lo estipulado en el documento "Política de seguridad".

6.8.3. Procedimiento de Actuación ante la Vulnerabilidad de la Clave Privada de una Autoridad de Certificación

El plan de contingencias de la jerarquía de Security Data Seguridad en Datos y Firma Digital trata el compromiso de la clave privada de la AC como un desastre.

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

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

6.8.4. Continuidad del Negocio después de un desastre

La AC restablecerá los servicios críticos (Revocación y publicación de certificados revocados) de acuerdo con esta DPC dentro de las 24 horas posteriores a un desastre o emergencia imprevista tomando como base el plan de contingencias y continuidad de negocio existente.

La AC dispone de un centro alternativo, en caso de ser necesario, para la puesta en funcionamiento de los sistemas de certificación.

6.9. Cese de Actividad

6.9.1. Autoridad de Certificación

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

- Proveerá de los fondos necesarios (para continuar la finalización de las actividades de revocación hasta el cese definitivo de la actividad, si es el caso.
- Informará a todos los suscriptores, solicitantes, usuarios, otras AC's o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el
- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los certificados, especificando, en su caso, si se va a transferir la gestión y a quien.

6.9.2. Autoridad de Registro

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

- Dejará de emitir y renovar certificados de ese Tercero Vinculado.
- Revocará los certificados de operador de ese Tercero Vinculado.
- Revocará los certificados de suscriptor emitidos por ese Tercero Vinculado salvo que expresamente se decida lo contrario.

7. CONTROLES DE SEGURIDAD TÉCNICA

7.1. Generación e Instalación del Par de Claves

7.1.1. Generación del Par de Claves

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

a) En hardware (soporte físico)

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

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

b) En software/Roaming

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

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

7.1.2. Entrega de la Clave Privada al Suscriptor

a) En hardware (soporte físico)

La clave privada será entregada junto al certificado en el dispositivo de creación de firma. El Tercero Vinculado será responsable de garantizar la entrega del dispositivo al suscriptor, asegurándose así que éste último está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

El dispositivo criptográfico utiliza una clave de activación para el acceso a las claves privadas o a su vez se accederá a este por medio de la huella digital en caso de disponer de un dispositivo biométrico.

b) En software

El suscriptor generará el par de claves directamente en su sistema y se guardará en el CAPI del computador.

c) Roaming

El suscriptor generará el par de claves directamente en su sistema y se almacena en los servidores de Security Data.

7.1.3. Entrega de la Clave Pública al Emisor del Certificado

El envío de la clave pública a la AC para la generación del certificado se realiza mediante un formato estándar preferiblemente en formato PKCS#10 o X.509 autofirmado, utilizando un canal seguro para la transmisión.

7.1.4. Entrega de la Clave Pública de la AC a los Terceros que Confían en los Certificados

El certificado de las ACs de la cadena de certificación y su fingerprint (huella digital) estarán a disposición de los usuarios en la página web de Security Data Seguridad en Datos y Firma Digital.

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

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

Los usos admitidos de la clave para cada certificado están definidos en la Política de Certificación correspondiente.

7.1.5.1. Extended Key Usage (EKU)

Los EKUs que se incluyen en los Certificados de Firma Electrónica de Security Data S.A. son los siguientes:

Server Auth	1.3.6.1.5.5.7.3.1
Client Auth	1.3.6.1.5.5.7.3.2
OCSP	1.3.6.1.5.5.7.4
Timestamping	1.3.6.1.5.5.7.3.88.1

7.2. Protección de la Clave Privada y Controles de Ingeniería de los Módulos Criptográficos

7.2.1. Estándares para los Módulos Criptográficos

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

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

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

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

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

7.2.3. Custodia de la Clave Privada

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

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

7.2.4. Copia de Seguridad de la Clave Privada

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

Las claves de la AC Raíz y AC Subordinada se pueden restaurar por un proceso que requiere la utilización simultánea de 3 de 5 dispositivos criptográficos (tarjetas).

Este procedimiento se describe en detalle en las políticas de seguridad de Security Data Seguridad en Datos y Firma Digital.

7.2.5. Archivo de la Clave Privada

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 dispositivo de creación de firma u otros métodos, 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.

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

Existe un documento de ceremonia de claves de la AC donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

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

7.2.7. Método de Activación de la Clave Privada

Las claves de la AC Raíz se activan por un proceso que requiere la utilización simultánea de 3 de 5 dispositivos criptográficos (tarjetas). Las claves de las AC Subordinadas se activan por un proceso que requiere la utilización de 1 de 4 dispositivos criptográficos (tarjetas).

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

7.2.8. Método de Desactivación de la Clave Privada

La clave privada del suscriptor de certificados con DSCF quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura.

7.2.9. Método de Destrucción de la Clave Privada

Se destruirán físicamente o reinicializarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de la clave privada de firma de certificados de las ACs, o de los datos de activación de las mismas.

7.3. Otros Aspectos de la Gestión del Par de Claves

7.3.1. Archivo de la Clave Pública

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

7.3.2. Periodos Operativos de los Certificados y Periodo de uso para el 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 la parte confiante pueda usarlo para verificar datos históricos teniendo en cuenta que no existirá un servicio de verificación en línea válido para ese certificado.

7.4. Datos de Activación

7.4.1. Generación e Instalación de los Datos de Activación

Los datos de activación son generados en el momento de inicialización del dispositivo criptográfico.

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

7.4.2. Protección de los Datos de Activación

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

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

7.5. Controles de Seguridad informática

La AC emplea sistemas fiables y productos comerciales para ofrecer sus servicios de certificación.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Security Data Seguridad en Datos y Firma Digital en los siguientes aspectos:

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

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

7.5.1. Requerimientos Técnicos de Seguridad Específicos

Cada servidor de la AC incluye las siguientes funcionalidades:

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

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

7.5.2. Evaluación de la Seguridad Informática

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

La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal es fácil debido al reducido número de personas que realizan sus trabajos en el centro de datos de Security Data Seguridad en Datos y Firma Digital.

7.6. Controles de Seguridad del Ciclo de vida

7.6.1. Controles de Desarrollo de Sistemas

La AC posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

7.6.2. Controles de Gestión de Seguridad

7.6.2.1. Gestión de Seguridad

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

La AC exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

7.6.2.2. Clasificación y Gestión de Información y Bienes

La AC mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de la AC detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, INTERNO y CONFIDENCIAL.

7.6.2.3. Operaciones de Gestión

La AC dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En la documentación técnica de la AC y de procedimientos del CPD se desarrolla en detalle el proceso de gestión de incidencias.

La AC dispone de cajas de seguridad ignífugas para el almacenamiento de soportes físicos.

La AC tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

7.6.2.4. Tratamiento de los Soportes y Seguridad

Todos los soportes serán tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

7.6.2.5. Planning del Sistema

El departamento técnico de la AC mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

7.6.2.6. Reportes de Incidencias y Respuesta

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

7.6.2.7. Procedimientos Operacionales y Responsabilidades

La AC define actividades asignadas a personas con un rol de confianza distinto a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

7.6.2.8. Gestión del Sistema de Acceso

La AC realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el acceso al sistema está limitado a las personas autorizadas. En particular:

a) Gestión general de la AC:

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

b) Generación del certificado:

- Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

- La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la AC.

c) Gestión de la revocación:

- Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular al sistema de revocaciones.
- La revocación se refiere a la perdida de efectividad de un certificado digital de forma Permanente. La revocación se realizara mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de AC.

d) Estado de la revocación

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

7.6.2.9. Gestión del Ciclo de Vida del Hardware Criptográfico

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

7.7. Controles de Seguridad de la Red

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

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

8. PERFIL DE LOS CERTIFICADOS

8.1. Perfil de los Certificados

El perfil de los certificados se corresponde con el propuesto en las políticas de certificación correspondientes, y son coherentes con lo dispuesto en las normas siguientes:

- ETSI TS 101 862 conocida como “European profile for Qualified Certificates”
- RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile",
- RFC 3739 “Qualified Certificates Profile”.

El perfil común a todos los certificados es el siguiente:

Campo del certificado	Nombre	Descripción
Versión	Nº de versión	V3 (versión del estándar X509)
Serial number	nº de serie	Código único con respecto al nombre distinguido del emisor
Signature Algorithm	Algoritmo de firma	Algoritmo de firma sha256RSA
Signature hash Algorithm	Algoritmo HASH de firma	Sha256
Issuer	Emisor	DN de la CA que emite el certificado
Valid from	Válido desde	Fecha de inicio de validez, tiempo UTC
Valid to	Válido hasta	Fecha de fin de validez, tiempo UTC
Subject	Sujeto	Nombre distinguido del suscriptor.
Public Key	Clave pública	Clave pública del suscriptor
Key Usage	Uso de la clave	Extensiones de los certificados.
Access to authority information	Acceso a información de autoridad	Información que indica que se utilizará OCSP
Certificate policies	Directivas del certificado	Información detallada del certificado incluyendo link a la PC del certificado

8.1.1.Número de Versión

Los certificados siguen el estándar X.509 versión 3.

8.1.2.Extensión de los Certificados

Las extensiones aquí presentadas corresponden con todas las que pueden contener los certificados emitidos. En la política de certificación de cada tipo de certificado se especificará las extensiones requeridas.

Extensión	Crítica	Posibles Valores
X509v3 Key Usage	Sí	Digital Signature Non Repudiation Key Encipherment, Data Encipherment, Key Agreement
X509v3 Authority Information Access	-	URI dónde se encuentra el certificado de la CA
X509v3 Certificate Policies	-	OID de la política de certificación correspondiente al certificado. URI de la CPS User Notice : Nota de texto que se puede desplegar en la pantalla del usuario
1.3.6.1.4.1.37746.2.1		Políticas de Certificado – Persona Natural
1.3.6.1.4.1.37746.2.2		Políticas de Certificado – Persona Jurídica-Empresa
1.3.6.1.4.1.37746.2.3		Políticas de Certificado – Representante Legal
1.3.6.1.4.1.37746.2.4		Políticas de Certificado – Miembro de Empresa
1.3.6.1.4.1.37746.2.5		Políticas de Certificado – Funcionario Público
1.3.6.1.4.1.37746.2.6		Políticas de Certificado – SSL
1.3.6.1.4.1.37746.2.7		Tipo de Certificado Persona Natural
1.3.6.1.4.1.37746.2.8		Tipo de Certificado Persona Jurídica
1.3.6.1.4.1.37746.2.9		Tipo de Certificado representante Legal
1.3.6.1.4.1.37746.2.10		Tipo de Certificado Miembro de Empresa
1.3.6.1.4.1.37746.2.11		Tipo de Certificado Funcionario Público
1.3.6.1.4.1.37746.2.12		Tipo de Certificado SSL
1.3.6.1.4.1.37746.2.13		Tipo de Certificado DEMO
1.3.6.1.4.1.37746.3.1		Cédula de ciudadanía o No. De Pasaporte

1.3.6.1.4.1.37746.3.2		Nombres
1.3.6.1.4.1.37746.3.3		Primer Apellido
1.3.6.1.4.1.37746.3.4		Segundo Apellido: (si no tiene queda en blanco)
1.3.6.1.4.1.37746.3.5		Cargo
1.3.6.1.4.1.37746.3.6		Institución
1.3.6.1.4.1.37746.3.7		Dirección
1.3.6.1.4.1.37746.3.8		Teléfono
1.3.6.1.4.1.37746.3.9		Ciudad
1.3.6.1.4.1.37746.3.10		Razón social
1.3.6.1.4.1.37746.3.11		RUC
1.3.6.1.4.1.37746.3.12		País
1.3.6.1.4.1.37746.3.26		Nombre del Representante Legal
1.3.6.1.4.1.37746.3.29		RUP
1.3.6.1.4.1.37746.3.27		Dominio
1.3.6.1.4.1.37746.3.28		Hora Legal del Ecuador
X509v3 Subject Alternative Name	-	email del suscriptor (o de la CA)
X509v3 CRL Distribution Points	-	URI de la CRL
X509v3 Private Key Usage Period	Si	Periodo de uso de la llave privada
X509v3 Authority Key Identifier	-	id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma
X509v3 Subject Key Identifier	-	id de la clave pública del certificado, obtenido a partir del hash de la misma
X509v3 Basic Constraints	Sí	2 valores posibles en función de si se trata de un certificado de CA: CA:FALSE CA:TRUE
1.2.840.113533.7.65.0	-	Extensión de la versión de entrust
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
Thumbprint algorithm	Si	Algoritmo de creación de huella del certificado
Thumbprint	Si	Huella del certificado

8.1.3.Formatos de nombre

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre del Suscriptor	Nombre y Apellidos del suscriptor,
CN, Common Name	Nombre de la CA	Nombres y Apellidos de la CA
OU, Organizational Unit	Unidad Organizacional	Entidad de Certificación de Información
O,Organization	Organización	Nombre de la AC
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto “ES”.

8.1.4.Perfil de la CRL

El perfil de las CRL’s se corresponde con el propuesto en las políticas de certificación correspondientes, y con el estándar X.509 versión 3 de la RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Las CRL’s son firmadas por la autoridad de certificación que ha emitido los certificados

8.1.5.Número de Versión

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

8.1.6.CRL y Extensiones

8.1.6.1. CRL de la Autoridad Raíz (AC Root)

CAMPOS	VALORES
Versión	2
Número de CRL	Número incremental
Algoritmo de firma	Sha1WithRSAEncryption
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempo UTC)
Fecha de próxima actualización	Fecha efectiva de emisión + 6 meses
Identificador de la clave de autoridad	Hash de la clave del emisor
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO

Lista de revocación de certificados (CRL) indirecta	NO
Entradas de la CRL	Nº de serie del certificado Fecha de revocación Código de razón

8.1.6.2. CRL de las Autoridades de Certificación Subordinadas

CAMPOS	VALORES
Versión	2
Número de CRL	Número incremental
Algoritmo de firma	Sha1WithRSAEncryption
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempo UTC)
fecha de próxima actualización	Fecha efectiva de emisión + 7 días
Identificador de la clave de autoridad	Hash de la clave del emisor
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO
Lista de revocación de certificados (CRL) indirecta	NO
Entradas de la CRL	Nº de serie del certificado Fecha de revocación Código de razón

9. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

9.1. Frecuencia de las Auditorias

Se realizarán auditorias periódicas, generalmente con carácter anual.

9.2. Cualificación del Auditor

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

9.3. 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 realiza auditorias periódicas internas a las AC de la jerarquía para garantizar en todo momento su adecuación a los requerimientos marcados por las políticas de certificación de la jerarquía.

9.4. 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
- La integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.

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.

9.4.1. Auditoría en las Autoridades de Registro

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

desarrollar por la Autoridad de Registro en cuanto a número de certificados o requerimientos específicos de seguridad.

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

9.5. Acciones a emprender como Resultado de la Detección de Incidencias

En caso de que sean detectadas incidencias o no-conformidades, se habilitarán las medidas oportunas para su resolución en el menor tiempo posible. Para no-conformidades graves (afectan a los servicios críticos, a saber, SERVICIOS DE REVOCACIÓN, SERVICIOS DE ACTIVACIÓN / SUSPENSIÓN DE CERTIFICADOS, SERVICIOS DE PUBLICACIÓN DE CRL), Security Data Seguridad en Datos y Firma Digital se compromete a su resolución en un plazo máximo de tres meses.

En todo caso se formará un comité de resolución formado por personal de las áreas afectadas y otro de seguimiento formador por los responsables de las áreas afectadas y Dirección General.

9.6. Comunicación de Resultados

El auditor comunicará los resultados al director técnico y al Director General, en tanto que responsable máximo de Security Data Seguridad en Datos y Firma Digital.

10.OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

10.1. Tarifas

10.1.1. 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 https://www.securitydata.net.ec

10.1.2. Tarifas de Acceso a los Certificados

El acceso a 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.

10.1.3. 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).

10.1.4. Tarifas de 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.

10.2. Confidencialidad de la Información

Security Data Seguridad en Datos y Firma Digital dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo que deberán firmar todas las personas que tengan acceso a información confidencial.

10.2.1. Ámbito de la Información Confidencial

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

10.2.2. Información no Confidencial

La siguiente información será considerada no confidencial:

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

10.2.3. Responsabilidad en la Protección de Información Confidencial

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

11.Revisiones

Documento: Declaración de Prácticas de Certificación								
Revisión	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Publicado	03/09/2011	31/03/2011	24/06/2011	01/09/2011	26/09/2011	13/12/2011	04/07/2011	13/09/2013
Autor(es)	LV/XC	XC	XC	DC/XC	XC	XC	XC	XC
Fecha de revisión	18/02/2011	16/05/2011		14/09/2011			04/07/2011	
Revisado por	XC	XC		XC				
Fecha aprobado	18/02/2010	16/05/2011		16/09/2011	26/09/2011	13/12/2011	04/07/2011	13/09/2013
Aprobado por	CS	CS	CS	CS	CS	CS	CS	CS