POLÍTICAS DE CERTIFICADOS (PC)

Certificado de

MIEMBRO DE EMPRESA

Versión 10.1

PC DE LA ECI SECURITY DATA

SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.

Contenido

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 ahora ARCOTEL

1.2. Vigencia

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

1.3. Soporte Legal

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

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

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

d) Que, el segundo artículo enumerado agregado por el artículo 4 del Decreto Ejecutivo No. 1356 a continuación del artículo 17 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, dispone que la acreditación como entidad de certificación de información y servicios relacionados, consistirá en un acto administrativo emitido por el CONATEL a través de

una resolución que será inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados.

e) 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.

f) 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 lo cual la SENATEL suscribió el respectivo acto administrativo, conforme el modelo aprobado por el Consejo Nacional de Telecomunicaciones.

2. INTRODUCCIÓN

2.1. Presentación

El presente documento contempla la Política de Certificación (PC) de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL para los Certificados de Miembro de Empresa

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

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

2.2. Nombre del Documento

2.2.1. Identificación

Nombre:	Políticas de Certificado (PC)
Versión:	10.0
Descripción:	Políticas de Certificado de Miembro de Empresa
Fecha de Emisión:	09 de septiembre 2021

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

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 (CertificateRevocationList)
HSM:	Módulo de seguridad criptográfico (Hardware Security Module)
LDAP:	LightweightDirectory 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 StampAuthority)
VA:	Autoridad de validación (ValidationAuthority)
ECI:	Entidad de Certificación de Información

OID:	Identificador de objeto único (Objectidentifier)
DN:	Nombre Distintivo (DinstinguishedName)
C:	País (Country), Atributo del Nombre Distintivo
CN:	Nombre Común (CommonName), Atributo del Nombre Distintivo
O:	Organización (Organization), Atributo del Nombre Distintivo
OU:	Unidad Organizacional (OrganizationalUnit), Atributo del Nombre
SN:	Apellido (SurName), Atributo del Nombre Distintivo
ISO:	International OrganizationalforStandarization
PKCS:	Public Key Cryptography Standars, Estándares PKI
UTF8:	Unicode TransformationFormat – 8 bits.

3. ENTIDADES PARTICIPANTES

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 y emisión de firmas electrónicas; y de sellado de tiempo, regidos por sus políticas particulares, no incluidas en este documento.

3.2. Autoridad de Certificación (AC)

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

3.2.1. Autoridades de Certificaciones Raíz

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

3.3. Autoridad de Registro (AR)

Una Autoridad de Registro (en inglés RA o RegistrationAuthority) de Security Data Seguridad en Datos y Firma Digital, es la entidad encargada de:

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

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

- Cualquier persona jurídica que sea cliente de Security Data Seguridad en Datos y Firma Digital, y cumpla el proceso para la acreditación para la emisión de certificados a nombre de la persona jurídica o a miembros de la misma.
- Cualquier entidad de confianza que llegue a un acuerdo con Security Data Seguridad en Datos y Firma Digital para actuar como intermediario en nombre de Security Data Seguridad en Datos y Firma Digital.
- La propia Security Data Seguridad en Datos y Firma Digital directamente.

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

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

Allí donde la ubicación geográfica de los suscriptores represente un problema logístico para la identificación del suscriptor y en la solicitud y entrega de certificados, la AR podrá delegar estas funciones a otra entidad de confianza. Dicha entidad deberá tener una especial vinculación con la AR y una relación de proximidad con los suscriptores de los certificados que justifique la delegación. La entidad de confianza deberá firmar un acuerdo de colaboración con la AR en el 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.

3.4. Solicitante

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

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

3.6. Firmante

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

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

3.7. Custodio de Claves

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

3.8. Tercero que confía en los Certificados

Se entiende como tercero que confía en los certificados (en inglés, relayingparty) 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 la DPC de Security Data Seguridad en Datos y Firma Digital.

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

4. CARACTERÍSTICAS DE LOS CERTIFICADOS

4.1. Período de validez de los certificados

Los certificados de Miembro de Empresa tendrán la vigencia elegida por el usuario en el formulario de solicitud, o por defecto dos años, hasta un máximo de cinco años contados a partir de la fecha de emisión del mismo de acuerdo al Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Decreto No.3469).

4.2. Tipos de Soporte

Los Certificados de Miembro de Empresa se podrán generar tanto en soporte de hardware o de Software.

4.3. 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 a la AR 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.

4.4. Soporte en Software

4.4.1. Certificados, llaves Públicas y privadas en Software

Este servicio permite al usuario, después de haber realizado la solicitud y que ésta haya sido aprobada por la Entidad Certificadora, se emita un certificado digital con sus llaves públicas y privadas, almacenándose en un archivo P12/PFX o como archivo EPF, el cual está protegido por una contraseña definida por el usuario, siendo el uso de estos certificados para firmar y encriptar documentos y para correo cifrado.

4.4.2. 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 mediante los mecanismos necesarios para verificación de la información, relacionar un dominio de Internet con una Persona Jurídica o un comerciante registrado y, una vez que haya generado la solicitud en el Servidor web, se procederá a la generación en un formato .CER/CRT/DER.

Siendo el uso de estos certificados para la implementación de servidores Web Seguros.

5. TIPOS DE CERTIFICADOS

5.1. Certificados de Persona Jurídica

Los Certificados de Persona Jurídica son certificados reconocidos de firma electrónica cuyo suscriptor es una persona jurídica (ya sea una empresa, una organización, o una Administración Pública):

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

5.2. Certificados de Persona Natural

Certificados de Persona Natural: Son certificados reconocidos de persona natural que identifican al suscriptor como una persona natural que pueden ser usados para este certificado 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.

5.3. 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.

6. CERTIFICADOS DE MIEMBRO DE EMPRESA

6.1. Aspectos Generales

6.1.1. Ámbito de Aplicación

Los certificados emitidos por la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL bajo esta PC, pueden utilizarse para creación de firmas electrónicas y para cifrado. Así mismo, pueden utilizarse como mecanismo de identificación ante servicios y aplicaciones informáticas.

Por ello les será de aplicación la legislación ecuatoriana referida a la firma electrónica

6.1.2. Datos en el Certificado

La información que se incluirá en el Certificado de Miembro de Empresa emitido por la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL será la siguiente:

Campos incluidos en el certificado		Descripción	
Version	Versión	Muestra la versión dentro del estándar X.509 (v3)	
Serial number	Número de Serie	Número de serie del certificado	
Signature Algorithm	Algoritmo de firma	Algoritmo de firma sha256RSA	
Signature hash algorithm	Algoritmo de firma para HASH	sha256	
Issuer	Emisor	Organizational Unit Name (OU)	Entidad de certificación de Información (ECI)
		Domain Component(DC)	Información del dominio (securitydata.net.ec)
		Organization Name (O)	Nombre de organización de certificación- Security Data Seguridad en Datos y Firma Digital
		Country Name (c)	país de autoridad de certificación- Ecuador (ec)
Valid from	Válido Desde	Fecha de emisión del certificado	
Valid to	Válido Hasta	Fecha de caducidad del certificado	
Subject	Firmante	Common Name (CN)	Nombre completo del suscriptor
		Organizational Unit Name (OU)	Entidad de certificación de Información (ECI)

		Organization Name (O)	Nombre de organización de certificación- Security Data Seguridad en Datos y Firma Digital
		Country Name (c)	país de autoridad de certificación- Ecuador (ec)
Public Key	Clave Pública	Clave Pública del Suscriptor	
Key Usage	Uso de clave	Identifica el uso que será aplicable	
Access to authority information	Acceso a información de autoridad	Información que indica que se utilizará OSCP	
Certificate Policy	Directivas del Certificado	Información detallada del certificado incluyendo link a la PC del certificado	
1.3.6.1.4.1.37746.3.1	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	1.3.6.1.4.1.37746.3.2	Nombres	
1.3.6.1.4.1.37746.3.3	1.3.6.1.4.1.37746.3.3	Primer Apellido	
1.3.6.1.4.1.37746.3.4	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	1.3.6.1.4.1.37746.3.5	Cargo	
1.3.6.1.4.1.37746.3.7	1.3.6.1.4.1.37746.3.7	Dirección	
1.3.6.1.4.1.37746.3.34	1.3.6.1.4.1.37746.3.34	Código Postal: (si no tiene queda en blanco)	
1.3.6.1.4.1.37746.3.8	1.3.6.1.4.1.37746.3.8	Teléfono	
1.3.6.1.4.1.37746.3.9	1.3.6.1.4.1.37746.3.9	Ciudad	
1.3.6.1.4.1.37746.3.12	1.3.6.1.4.1.37746.3.12	País	
1.3.6.1.4.1.37746.3.10	1.3.6.1.4.1.37746.3.10	Razón Social	
1.3.6.1.4.1.37746.3.11	1.3.6.1.4.1.37746.3.11	RUC	
1.3.6.1.4.1.37746.3.29	1.3.6.1.4.1.37746.3.29	RUP (si no tiene queda en blanco)	
1.3.6.1.4.1.37746.3.32	1.3.6.1.4.1.37746.3.32	Número de Factura	
1.3.6.1.4.1.37746.3.33	1.3.6.1.4.1.37746.3.33	Número de Serie del Token	
Subject Alternative Name	Nombre Alternativo del Firmante	correo electrónico del suscriptor	
CRL Distribution Points	Puntos de Distribución de la CRL	Puntos de distribución de CRL. Dirección donde se publica la lista de revocación de Certificados	
Private Key Usage Period	Periodos de uso de clave Privada	Tiempo en que estará vigente la clave privada	
Authority Key Identifier	Identificador de clave de entidad emisora	Extensión del estándar X509	
Subject Key Identifier	Identificador de clave	Extensión del estándar X509	

	de asunto	
Basic Contrains	Restricciones Básicas	Determina a qué está destinada la AC, la ruta de certificación como entidad final de ECI
Entrust Version Info	Información de Entrust	Información sobre la plataforma PKI
Thumbprint Algoritm	Algoritmo de identificación	Algoritmo de firma utilizado por la AC
Thumbprint	Huella Digital	Id de huella asociado al certificado

6.2. Uso particular de los certificados

6.2.1. Uso 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 la 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 prohibida cualquier alteración del certificado por parte del usuario.

- Los certificados de firma electrónica no podrán ser utilizados para acciones ilícitas, de acuerdo con lo establecido en la legislación ecuatoriana.
- Los certificados de firma electrónica 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

6.2.2. Uso 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 la Declaración de Practicas de Certificación y en esta 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.

6.2.3. Generación de las claves y del Certificado

El soporte para el almacenamiento de las claves y el certificado será un dispositivo criptográfico o por medio de software. El acceso al dispositivo criptográfico, donde se encuentra la clave privada, se realizará a través de contraseña (PIN) o a su vez a través de la huella digital en los dispositivos biométricos. El acceso al certificado en Software en archivo formato P12/PFX se realiza mediante contraseña (definida por el usuario final). Para realizar una firma electrónica es necesario introducir el PIN/Contraseña que únicamente debe conocer el Suscriptor o el escaneo de la huella digital,

6.3. Tarifas

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/wp-content/downloads/listas/lista_precios.pdf

6.31. Cambio de tarifas o excepciones

Los precios indicados en el punto 6.3, pueden ser sujetos a revisión o modificación sin previo aviso, por parte de gerencia o departamento comercial de Security Data, de igual manera los precios pueden ser variables teniendo cuenta promociones o normativas legales vigentes en el país.

6.3.2. Tarifas de Acceso a los Certificados

El acceso a los certificados emitidos será de acuerdo a lista de precios publicada de acuerdo a las tarifas contempladas en el listado del numeral 6.3

6.3.3. 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).

6.3.4. Tarifas de Otros Servicios

Las tarifas aplicables a otros se contemplaran en el listado de precios publicado de acuerdo al listado del numeral 6.3

6.3.5. Reembolsos

Los suscriptores de certificados podrán solicitar reembolso de dinero bajo los siguientes lineamientos:
Cuando se haya realizado un depósito en exceso
Cuando el servicio no ha sido proporcionado y el cliente no desea seguir con el tramite
Para estos casos el cliente deberá demostrar las evidencias del pago realizado, una vez analizadas las circunstancias para efectuar el reembolso el departamento financiero procederá con la devolución respectiva.

En estos casos el cliente debe enviar un correo electrónico indicando el motivo del reembolso a devoluciones@securitydata.net.ec, una vez analizado si aplica o no el reembolso se procede a comunicar al cliente
El valor del reembolso será el del servicio solicitado, y el valor depositado en exceso.

6.4. Solicitud de Certificados

6.4.1. Quién puede solicitar un certificado

Solicitante es la persona natural que identifica al suscriptor como persona jurídica y al firmante como vinculado a esa persona jurídica, ya sea como empleado, asociado, colaborador, cliente o proveedor, solicita la emisión de un certificado a Security Data Seguridad en Datos y Firma Digital. El solicitante o el suscriptor de un certificado de Miembro de Empresa deberá estar en posesión de la siguiente documentación:

a) Se realizará un proceso de biometría para validar la identidad del solicitante y en caso de extranjeros se solicitará el pasaporte; en caso de que el proceso de validación no fuera exitoso se procederá con la solicitud de la cedula de identidad, y un video del solicitante con un script definido por la entidad de certificación.
b) La entidad de certificación validara ante el SRI el RUC y almacenara una captura de pantalla del estado del mismo, en caso de que la pagina del SRI no se encuentre disponible, el certificado no se otorga hasta que se realice la validación manual del RUC.

c) Copia legible del nombramiento con su debida inscripción cuando corresponda o registro de directivas según el caso, del miembro de empresa en caso de Personas Jurídicas.
d) Copia de constitución, estatutos o documento de creación según corresponda de la Empresa solicitante.
e) Carta de autorización, nombramiento, o registro de directivas cuando corresponda según el caso.

6.4.2. Procesos de Solicitud de Certificado

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 AC, presencial, o a alguna de las ARs asociadas. La AR proporcionará al solicitante la siguiente información:

- Documentación necesaria para 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.

6.5. Tramitación de las Solicitudes de Certificados

6.5.1. Realización de las funciones de identificación y autenticación

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

6.5.2. Aprobaciones o denegación de las solicitudes de certificados

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

Si la información no es correcta, la AR denegará la petición, indicándole al solicitante el motivo. Si es correcta, se procederá a la firma del instrumento jurídico vinculante entre el suscriptor y/o el solicitante y Security Data Seguridad en Datos y Firma Digital.

6.6. Emisión de Certificados

6.6.1. Acciones de la AR

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.
• 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.
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:

Una vez recibido la notificación por correo electrónico por parte del suscriptor, tendrá que generar su certificado a través del portal indicado, llenando el formulario de descarga con los siguientes datos:
Número de cédula
Número de ruc (solo persona jurídica)
Número de referencia
Contraseña que el suscriptor creará en el momento de la descarga.

6.6.2. Entrega del certificado.

Cuando el suscriptor tenga las dos claves generadas (Código de Autorización y Número de Referencia, para emisión en Hardware), podrá generar el certificado.

a) 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.

b) En Software

Una vez recibido la notificación por correo electrónico por parte del suscriptor, tendrá que generar su certificado a través del portal indicado, llenando el formulario de descarga con los siguientes datos:
Número de cédula
Número de ruc (solo persona jurídica)
Número de referencia
Contraseña que el suscriptor creará en el momento de la descarga.

6.7. Aceptación del Certificado

6.7.1. 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 y el certificado haya sido entregado de acuerdo con el procedimiento seleccionado por el suscriptor.

Como evidencia de la aceptación se firma el contrato con el certificado electrónico, almacenándose en los servidores de la AC y enviado una copia al suscriptor mediante correo electrónico. El certificado se considerará válido a partir de la fecha en que se emite el certificado.

6.7.2. Publicación del Certificado

Una vez el certificado generado y aceptado por el suscriptor o firmante, el certificado será publicado en los repositorios de certificados de la AC.

6.8. 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.

6.8.1. 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 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

6.8.2. 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.

6.8.3. 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 de la misma.

6.8.3.1 Revocación en Horario de Oficina

El suscriptor o el firmante deberá ponerse en contacto con la entidad de certificación o el Tercero Vinculado de Security Data Seguridad en Datos y Firma Digital ya sea vía correo electrónico, personal o telefónicamente.
Si se asiste personalmente el suscriptor o firmante quedará autenticada mediante su cédula de identidad o pasaporte y se podrá proceder a la revocación inmediata del certificado, posterior al llenado de la solicitud de revocación y entregado al operador de autoridad de registro, en caso de suspensión el suscriptor puede solicitar previa validación de datos de la AC.
Si lo hace vía telefónica al 023922169-026020655-046020655, el certificado quedará suspendido hasta que el suscriptor o firmante se presenten personalmente ante el Tercero Vinculado o envíen una carta pidiendo la revocación del certificado. El certificado quedará suspendido por un periodo máximo de 90 días al cabo de los cuales éste será revocado. Dentro de estos 90 días el solicitante o firmante puede cancelar la suspensión y el procedimiento de revocación.
Si lo hace vía correo electrónico a soporte@securitydata.net.ec, el certificado quedará suspendido hasta que el suscriptor presente personalmente ante el tercer vinculado o envié una carta pidiendo la revocación del certificado, en caso de que la solicitud de revocación se encuentre firmada electrónicamente se procede con la revocación definitiva, caso contrario el certificado quedará suspendido por un periodo de 90 días al cabo de los cuales este será revocado. Dentro de estos 90 días el solicitante o firmante puede cancelar la suspensión y el procedimiento de revocación.
Dependiendo del tipo de solicitud receptada el operador realizará la revocación respectiva dentro del portal ingresos de Security Data,

misma que cuenta con la opción de revocación en la cual puede suspender o revocar el certificado previo a cargar la carta entregada por el suscriptor, por los diferentes medios antes citados.
Las revocaciones y suspensiones tienen efecto desde el momento en que aparecen publicadas en la CRL.

6.8.3.1.1 Criterios de suspensión

Un certificado podrá ser suspendido 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 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

6.8.3.1.2. Criterios de levantamiento de suspensión

El cliente será el único ente autorizado para el levantamiento de la suspensión, de acuerdo con criterio del suscriptor, y el mismo no podrá ser delegada a una tercera persona, el procedimiento para la suspensión o levantamiento es el mismo detallado en el punto 6.8.3.1.1

6.8.3.2. Revocación Fuera de Horario de Oficina

El cliente solicitará la revocación por correo electrónico a soporte@securitydata.net.ec, la misma será procesada el siguiente día hábil a partir de las 9h00.

6.8.4. 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.

6.8.5. 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.

6.8.6. 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.

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

6.8.7. 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.

6.8.8. 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.

6.8.9. 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.

6.8.10. 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 ARCOTEL, de conformidad en lo previsto en la ley de Comercio electrónico, firmas electrónicas y mensajes de datos
- Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado.
- Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

6.8.11. 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.

6.8.12. Límites del Periodo de Suspensión

El límite lo establece el cliente mismo o a su vez la validez del certificado o lo descrito en el punto 6.8.3.1.2.

6.8.12. Circunstancias para el levantamiento de la suspensión

El suscriptor es quien solicitará el levantamiento de la suspensión previo a los 90 días caso contrario el certificado será revocado.

6.9. Renovación de certificados

6.9.1. Renovación de Certificados sin Cambio de Claves

No se contempla esta opción.

6.9.2. Renovación con Cambio de Claves

Proceso de renovación, que se efectuará del mismo modo que la emisión de un nuevo certificado, ya que el suscritor tiene en su posesión la llave pública y privada, por tal motivo la entidad de certificación no almacena dicha información y se emite un nuevo certificado y por ende no puede extender la vigencia del certificado sin una nueva emisión del mismo.

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

6.10.1. Estándares para los Módulos Criptográficos

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

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

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

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

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

6.10.3. Custodia de la Clave Privada

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

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

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

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

Las claves de la AC Raíz se pueden restaurar de acuerdo con lo indicado en el Procedimiento de Recuperación, respaldo y almacenamiento de claves privadas

de la AC.

6.10.5. Archivo de la Clave Privada del Suscriptor

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

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

Las claves privadas de los suscriptores pueden ser archivadas por ellos mismos, mediante la conservación del 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.

6.10.6. 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.

6.10.7. 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.

6.10.8. 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.

6.10.9. Método de Destrucción de la Clave Privada

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

6.11. Notificación de caducidad de certificado a un suscriptor para su renovación

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

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

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

Security Data notificará a las entidades, organismos del gobierno y empresas privadas la renovación de un certificado por medio de la página Web de Security Data.

7. REVISIONES

Documento: Políticas de Certificado Miembro de Empresa								
Revisión	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Publicación	24/01/2011	31/03/2011	27/06/2011	01/09/2011	26/09/2011	15/12/2011	25/02/2015	25/06/2019
Autor(es)	LV/XC	XC	XC	XC	XC	XC	DC	DC/LV
Fecha Revisión	18/02/2011	16/05/2011	16/05/2011	14/09/2011			05/03/2011	25/06/2011

Revisado Por	XC	XC	XC	XC	XC	XC	CS	LV
Fecha Aprobado	02/03/2011	16/05/2011	16/08/2011	15/09/2011	26/09/2011	15/12/2011	05/03/2015	25/06/2011
Aprobado Por	CS	CS	CS	CS	CS	CS	CS	CS

CESAR NAPOLEON SANTANA VILLAMAR
Firmado digitalmente por CESAR NAPOLEON SANTANA VILLAMAR
Fecha: 2022.08.24 09:46:39 -05'00'