POLÍTICAS DE CERTIFICADO
(PC)

Certificado de Funcionario Público
Versión 7.0

PC DE LA
ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, S.A.

Contenido

1. MARCO LEGAL 5
1.1. Base Legal 5
1.2. Vigencia 5
1.3. Soporte Legal 5
2. INTRODUCCIÓN 6
2.1. Presentación 6
2.2. Nombre del Documento 6
2.2.1. Identificación 6
2.2.2. Publicación 7
2.3. Definiciones y Acrónimos 7
2.3.1. Definiciones 7
2.3.2. Acrónimos 8
3. ENTIDADES PARTICIPANTES 10
3.1. Entidad Acreditada (EA) 10
3.2. Autoridad de Certificación (AC) 10
3.2.1. Autoridad de Certificación Raíz 10
3.3. Autoridad de Registro (AR) 10
3.4. Solicitante 12
3.5. Suscriptor 12
3.6. Firmante 12
3.7. Custodio de las Claves 12
3.8. Tercero que confía en los Certificados 12
4. CARACTERÍSTICAS DE LOS CERTIFICADOS 13
4.1. Periodo de validez de los certificados 13
4.2. Tipos de soporte 13
4.3. Dispositivo Seguro de Creación de Firma (DSCF) 13
4.4. Soporte en Software 14

4.4.1. Certificados, llaves Públicas y privadas en Software 14
4.4.2. Certificados, llaves públicas y privadas para Servidor Web Seguro – SSL 14
4.5. Soporte en Roaming 15
5. TIPOS DE CERTIFICADOS 15
5.1. Certificados Corporativos Reconocidos 15
5.2. Certificados para la Administración Pública 15
5.3. Certificados Privados 16
5.4. Certificados de Servidor Seguro 16
6. CERTIFICADO DE FUNCIONARIO PÚBLICO 16
6.1. Aspectos Generales 16
6.1.1. Ámbito de Aplicación 16
6.1.2. Datos en el Certificado 16
6.2. Uso particular de los certificados 18
6.2.1. Usos apropiados de los certificados 18
6.2.2. Usos no autorizados de los certificados 19
6.2.3. Generación de las Claves y del Certificado 19
6.3. Tarifas 20
6.4. Solicitud de Certificados 20
6.4.1. Quién puede solicitar un Certificado 20
6.4.2. Procesos de Solicitud de Certificado 21
6.5. Tramitación de las Solicitudes de Certificados 21
6.5.1. Realización de las funciones de identificación y autenticación 21
6.5.2. Aprobación o denegación de las solicitudes de certificados 21
6.6. Emisión de Certificados 22
6.6.1. Acciones de la AR 22
6.6.2. Acciones de la AC 22
6.6.3. Emisión del certificado 22
6.7. Aceptación del Certificado 23

6.7.1. Forma en la que se acepta el Certificado 23
6.7.2. Publicación del Certificado 23
6.8. Revocación y Suspensión de Certificados 24
6.8.1. Supuestos de revocación 24
6.8.2. Causas para la revocación 24
6.8.3. Quién puede Solicitar la Revocación 25
6.8.4. Procedimientos de Solicitud de Revocación 26
6.8.5. Plazo en el que la AC debe Resolver la Solicitud de Revocación 27
6.8.6. Obligación de Verificación de las Revocaciones por los Terceros 27
6.8.7. Frecuencia de Emisión de CRL 27
6.8.8. Tiempo Máximo entre la Generación y la Publicación de las CRL 28
6.8.9. Disponibilidad del Sistema en Línea de Verificación del Estado de los Certificados 28
6.8.10. Requisitos de Comprobación de Revocación en Línea 28
6.9. Renovación de certificados 28
6.9.1. Circunstancias para la Suspensión 29
6.9.2. Quién puede Solicitar la Suspensión 29
6.9.3. Límites del Periodo de Suspensión 29
7. Revisiones 30

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

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 Funcionario Público.

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 7.0
Descripción:	Políticas de Certificado de Funcionario Público.
Fecha de Emisión:	22 de Septiembre 2015

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 Distintivo
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 CertificateAuthority) organizadas bajo una Jerarquía de Certificación.

3.2.1. Autoridad de Certificación Raíz

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

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 Corporación que sea cliente de Security Data Seguridad en Datos y Firma Digital, para la emisión de certificados a nombre de la corporación o a miembros de la corporación.
- 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 Corporación (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 las 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. Periodo de validez de los certificados

Los certificados de Funcionario Público tendrán la vigencia elegida por el usuario en el formulario de solicitud, de acuerdo al nombramiento, o por defecto dos años, hasta un máximo de seis 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 Funcionario Público 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 y luego de haber recibido los códigos de generación, acceder al portal de Security Data para 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.

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, relacionar un dominio de Internet con una Funcionario Público o un comerciante registrado y una vez haya recibido los códigos de generación, pueda acceder 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.

4.5. 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 AC. Este repositorio es seguro con doble capa de encripción 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.

5. TIPOS DE CERTIFICADOS

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: Son certificados reconocidos de persona jurídica que identifican al suscriptor como Funcionario Público,
- 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.

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.

- Certificados Corporativos de Funcionario Público: Son certificados reconocidos de persona natural que identifican al suscriptor como una corporación y al firmante como representante legal de dicha corporación.

5.3. Certificados Privados

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.

5.4. 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.

6. CERTIFICADO DE FUNCIONARIO PÚBLICO

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 Funcionario Público 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	Algoritmo HASH de firma	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	Sujeto	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	
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)	
1.3.6.1.4.1.37746.3.1	1.3.6.1.4.1.37746.3.1	Cédula de ciudadanía o No. De Pasaporte	
1.3.6.1.4.1.37746.3.5	1.3.6.1.4.1.37746.3.5	Cargo	
1.3.6.1.4.1.37746.3.10	1.3.6.1.4.1.37746.3.10	Razón social	
1.3.6.1.4.1.37746.3.7	1.3.6.1.4.1.37746.3.7	Dirección	
1.3.6.1.4.1.37746.3.9	1.3.6.1.4.1.37746.3.9	Ciudad	

1.3.6.1.4.1.37746.3.8	1.3.6.1.4.1.37746.3.8	Teléfono
1.3.6.1.4.1.37746.3.11	1.3.6.1.4.1.37746.3.11	RUC (de la institución)
1.3.6.1.4.1.37746.3.10	1.3.6.1.4.1.37746.3.12	País
1.3.6.1.4.1.37746.3.6	1.3.6.1.4.1.37746.3.6	Institución
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 de	Extensión del estándar X509
Basic Constrains	Restricciones Básicas	Determina a qué está destinada la AC, la ruta de
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. 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 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 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.

6.2.2. Usos no autorizados de los certificados

No se permite el uso que sea contrario a la normativa ecuatoriana y comunitaria, a los convenios internacionales ratificados por el estado ecuatoriano, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en 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. Para realizar una firma electrónica es necesario introducir el PIN que únicamente debe conocer el Suscriptor o de escanear la huella digital. En la generación de las claves no se permite realizar

una copia de seguridad de las mismas.

6.3. Tarifas

El precio de los certificados Corporativos de Miembro de Empresa dependerá de la duración de los mismos.
Security Data Seguridad en Datos y Firma Digital S.A podrá establecer las tarifas que considere oportunas a los suscriptores, así como establecer los medios de pago que considere más adecuado en cada caso. Para más detalles sobre el precio y condiciones de pago de este tipo de certificados será necesario consultar con Security Data Seguridad en Datos y Firma Digital S.A.

6.4. Solicitud de Certificados

6.4.1. Quién puede solicitar un Certificado

Persona natural que identifican al suscriptor como una Administración Pública y al firmante como empleado de la misma que solicita la emisión de un certificado a Security Data Seguridad en Datos y Firma Digital. El solicitante o el suscriptor de un certificado de Funcionario Público deberán estar en posesión de la siguiente documentación:

a) Cédula de ciudadanía o pasaporte en casos de extranjeros,
b) Papeleta de votación actualizada, (para extranjeros, certificado de empadronamiento y para militares copia de la libreta militar).
c) Original o copia certificada y legible del nombramiento o "Acción de Personal" del solicitante o a su vez un certificado laboral que certifique el cargo del Funcionario Público, actualizado, firmado por el representante legal o emitida por el departamento de recursos humanos de la institución.
d) Registro único de contribuyentes (RUC) de la institución
e) Registro único de proveedores (RUP) en caso de disponerlo
f) Original o copia certificada y legible del nombramiento del representante legal adjuntando copia clara de la cédula de ciudadanía del mismo en caso de Personas Jurídicas
g) Autorización firmada por el representante legal, donde conste el número de solicitudes, nombre y cargo de todos los solicitantes de la Empresa

para emisión de certificado de Firma Electrónica.

h) Ser persona natural y mayor de edad.

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 o a alguna de las ARs asociadas. La AR 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 los siguientes puntos se especifica la documentación requerida para la solicitud de este certificado.

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. Aprobación 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 la AR notificará al suscriptor y/o el solicitante, el mismo que deberá:

a) Identificarse presencialmente ante la AR, según el procedimiento que ésta le comunique.
b) Pagar el valor de los certificados o presentar el comprobante de pago a la AR (Software o Hardware).
c) Leer, aceptar y firmar la Hoja de Entrega y Aceptación (Contrato), que quedará en poder de la AR y el firmante podrá obtener una copia.
d) Si el Suscriptor requiere el Certificado vía Hardware y no dispone de Token AR hará entrega del mismo y cuando el solicitante aporte su propio dispositivo, éste deberá ser homologado por Security Data Seguridad en Datos y Firma Digital previamente a su utilización. Las ARs dispondrán de una lista de dispositivos homologados.
e) La AR ingresará los datos en el sistema y procederá a emitir los códigos de generación de certificados, los mismos que serán entregados de la siguiente forma: El primero llamado Número de Referencia será enviado al correo electrónico del solicitante y el segundo llamado Código de Autorización se entregará impreso en ese momento al solicitante, en conjunto con la Factura.

6.6.2. Acciones de la AC

Una vez aprobada la solicitud se procederá a la emisión del certificado.

6.6.3. Emisión 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 en el enlace de EMISIÓN y deberá seguir el procedimiento que se describe en el Manual de Activación del Certificado vía Software que se encuentra en la página web https://www.securitydata.net.ec. Una vez realizado el procedimiento se emite el certificado, el mismo que se instalará el solicitante en su computador o si es que se trata de roaming, éste se instalará en los servidores de Security Data S.A

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 que se encuentra en la página web https://www.securitydata.net.ec Una vez realizado el procedimiento se emite el certificado, el mismo que se instalará el Token.

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 físicamente, ya sea personal o por algún medio seguro.

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 a la AR físicamente.

6.7.2. 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.

6.8. Revocación y Suspensión de Certificados

6.8.1. Supuestos de revocación

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.

6.8.2. 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 de la AR, 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.

f) 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. 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 de la AR a la que pertenece el suscriptor del certificado.
- Los operadores autorizados de la AC.
- Los mismos usuarios accediendo a la administración de su certificado

6.8.4. 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 una notificación al suscriptor, comunicando la hora y la causa de la misma.

6.8.4.1. 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 (Revoke)
- Introducir la causa de revocación.

Una vez aceptado, el certificado será inmediatamente revocado.

6.8.4.2. Revocación en Horario de Oficina

El suscriptor o el firmante deberá ponerse en contacto con la AR 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 la AR 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 a la AR y al cliente con los datos de suspensión y/o revocación y el motivo.

6.8.4.3. Revocación Fuera de Horario de Oficina

Ver 6.8.4.1 Procedimiento Online

6.8.5. 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 la AR, la revocación se hará efectiva inmediatamente.

6.8.6. 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.

6.8.7. Frecuencia de Emisión de CRL

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 se emite cada 6 meses o cuando se produzca una revocación.

6.8.8. 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.

6.8.9. 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.

6.8.10. Requisitos de Comprobación de Revocación en Línea

Para el uso del servicio de CRLs, que es de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión "CRL Distribution Point".
- El usuario deberá comprobar adicionalmente la(s) CRL(s) pertinentes de la cadena de certificación de la jerarquía.
- El usuario deberá asegurarse que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.
- Los certificados revocados que expiren serán retirados de la CRL.

6.9. Renovación de certificados

Existen dos procedimientos:

a) Proceso de renovación presencial: El suscriptor deberá dirigirse a Security Data Seguridad en Datos y Firma Digital S.A, y proceder a la generación de un certificado nuevo.
b) Proceso de renovación online: Si se dispone del servicio y el suscriptor ha contratado la renovación, éste recibirá una notificación de Security Data Seguridad en Datos y Firma Digital S.A por correo electrónico para iniciar la renovación a través de la página web de Security Data Seguridad en Datos y Firma Digital S.A.

6.9.1. 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.

6.9.2. Quién puede Solicitar la Suspensión

Solamente podrán realizar la suspensión del certificado:

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

6.9.3. Límites del Periodo de Suspensión

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

7. Revisiones

Documento: Políticas de Certificado Funcionario Público							
Revisión	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Publicado	**24/01/2011**	**31/03/2011**	**27/06/2011**	**01/09/2011**	**26/09/2011**	**15/12/2011**	**18/09/2015**
Autor(es)	**LV/XC**	**XC**	**XC**	**XC**	**XC**	**XC**	**DC**
Fecha de revisión	**18/02/2011**	**16/05/2011**	**27/06/2011**	**14/06/2011**			
Revisado por	**XC**	**XC**	**XC**	**XC**			**XC**
Fecha aprobado	**02/03/2011**	**16/05/2011**	**16/08/2011**	**16/09/2011**	**26/09/2011**	**15/12/2011**	**18/09/2015**
Aprobado por	**CS**	**CS**	**CS**	**CS**	**CS**	**CS**	**CS**