DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Índice

1 Introducción

1.1. Presentación general del documento

El presente documento establece los lineamientos a seguir por parte de la Unidad de Firma Electrónica del Ministerio de Economía para la prestación de servicios como Autoridad de Certificación relacionados con la jerarquía raíz de El Salvador que incluye la emisión de certificados digitales de proveedores de servicios de certificación.

En el documento se detallan las prácticas a seguir en la aprobación, emisión, gestión de certificados (incluyendo publicación y archivo), revocación, renovación, suspensión, rehabilitación y demás prácticas del ciclo de vida del certificado.

Esta Declaración de Prácticas de Certificación recoge las normas que se emplean dentro de la autoridad de certificación vinculados al ciclo de vida de los certificados digitales y los controles para garantizar el servicio.

1.2. Referencias

La presente Declaración de Prácticas de Certificación (DPC) está fundamentada en las siguientes recomendaciones contenidas en:

Normas CEN EN 419 221: Parte de 2-5, según corresponda requisitos de seguridad para módulos criptográficos HSM.

ETSI EN 319 411 Part 1: Firma Electrónica e Infraestructuras, Requisitos de política y seguridad para proveedores de servicios de certificación que emiten certificados, Requerimientos Generales.

- sección 6.5.2 de ETSI EN 319 411-1 – Relacionada con módulos criptográficos.

ETSI EN 319 411 Part 2: Firma Electrónica e Infraestructuras, Requisitos de política y seguridad para proveedores de servicios de certificación que emiten certificados, Requerimientos para proveedores de servicios de certificación que emiten certificados digitales.

ETSI EN 319 412-1: Firma Electrónica y Infraestructuras, Perfiles de Certificados, Visión general y estructuras de datos comunes.

FIPS 140-2 nivel 3: valida el cumplimiento de su estándar PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, bajo su programa de validación Cryptographic Module Validation Program (CMVP).

ISO/IEC 19790 nivel 3: especifica los requerimientos de seguridad para un módulo criptográfico utilizado dentro de un sistema de seguridad que protege información sensible en sistemas informáticos y de telecomunicaciones.

1.3. Base Legal

[DECRETO133-2015]	Decreto No. 133. Ley de Firma Electrónica. Dada en el Salón Azul del Palacio Legislativo, en San Salvador, al 1 de octubre de 2015.
[DECRETO60-2016]	Decreto No. 60. Reglamento de la Ley de Firma Electrónica. Dado en Casa Presidencial, en San Salvador, al 10 de diciembre del 2016.

1.4. Nombre del documento e identificación

Este documento se denomina Declaración de Políticas de Certificación, el cual contiene la siguiente información que podrá ser consultada en la página web, de acuerdo a la siguiente información:

Nombre del documento	***DECLARACIÓN DE PRÁCTICAS DE CERTICACIÓN JERARQUÍA RAÍZ EL SALVADOR***
Identificador OID	*1.3.6.1.4.1.50377.2.1.1*
Versión	*1.0*
Fecha de emisión	*08/09/2020*
Ubicación	*http://normativa.firmaelectronica.economia.gob.sv/dpc/*

1.5. Participantes de la PKI

La Unidad de Firma Electrónica del Ministerio de Economía es la Autoridad Nacional para la administración de PKI en El Salvador, a cargo de la administración del mercado y el marco de servicios de certificación, y sus proveedores.

Los participantes con los que cuenta la jerarquía de certificación en El Salvador:

- Autoridad de Certificación (AC) Raíz
- Autoridad de Certificación (AC) Subordinada – Proveedor de servicios de certificación

- Autoridad de Registro AR
- Autoridad de Validación AV
- Autoridad de Sellado de Tiempo TSA
- Suscriptores de certificados
- Terceros que confían

A continuación, se describen las siguientes especificaciones para cada una de las entidades participantes:

1.5.1. Autoridades de Certificación (AC)

La Autoridad de Certificación es la entidad responsable de emitir y gestionar certificados digitales, garantizar la autenticidad y veracidad de los datos recogidos en el certificado digital expedido, actuar como tercera parte de confianza entre el suscriptor y un usuario de un certificado.

AC Raíz: Autoridad de Certificación de primer nivel, esta AC sólo emite certificados para sí misma y su(s) AC Subordinada(s) que serán los proveedores de servicios de certificación acreditados en El Salvador. Únicamente estará en funcionamiento durante la generación del certificado autofirmado; de certificados de AC Subordinada y periódicamente para la generación de la lista de certificados revocados de autoridad de certificación raíz ARL.

Los certificados de AC Subordinada podrán una duración máxima de 15 años.

AC Subordinada: Autoridad de Certificación subordinada de proveedores de servicios de certificación, su función es la emisión de certificados de usuario final de los siguientes tipos:

- Certificado de Persona Natural:
  - PN en calidad de ciudadano
  - PN en calidad de perteneciente a Empresa u Organización
  - PN profesional
  - PN Funcionario Público

- Certificado de Persona Natural Representante:
  - Representante legal de Persona Natural
  - Representante legal de la Persona Jurídica

- Certificado de Sello Electrónico
  - Empresa o Institución

- Certificado de Facturación electrónica
- Certificado de Sello de Tiempo
- Certificado de Respondedor OCSP

Los certificados Entidad Final emitidos por las Autoridades de Certificación Subordinadas podrán tener una duración máxima de 5 años.

1.5.2. Autoridad de Registro (AR)

La Autoridad de Registro es la entidad delegada por el proveedor de servicios de certificación, Autoridad de Certificación Subordinada acreditada dentro de El Salvador de la identificación y autenticación de los solicitantes de certificados de usuario final, con el fin de receptar y procesar las solicitudes de certificados digitales.

Está facultada además para solicitar a la AC Subordinada la revocación, suspensión, rehabilitación y renovación de certificados.

La Autoridad de Registro llevará un registro completo de los solicitantes que ingresen una solicitud para obtener un certificado, guardando un archivo de las mismas.

1.5.3. Autoridad de Validación (AV)

La Autoridad de Validación proporciona el servicio para la validación de los certificados de entidad final emitidos por la AC Subordinada a través del protocolo de consulta en línea de estado de certificados OCSP conforme al estándar RFC 2560.

Las respuestas OCSP están firmadas con la clave privada correspondiente al certificado de respondedor OCSP de la Autoridad de Validación emitido por el Proveedor de servicios de certificación.

1.5.4. Autoridad de Sellado de Tiempo (TSA)

La Autoridad de Sellado de Tiempo proporciona el servicio de emisión de tokens de sellado de tiempo (TST), que indica que una firma o certificado o dato ha existido y no ha sido alterado desde un instante específico en el tiempo, a través del protocolo TSP conforme al estándar RFC 3161.
La sincronización de la hora de los equipos de la AST de los entornos de producción, contingencia y pruebas se la realiza mediante el protocolo de sincronización de tiempo en red NTP ofrecido por el Centro de Investigaciones de Metrología.

Los sellos de tiempo emitidos están firmados con la clave privada correspondiente al certificado de sellos de tiempo emitidos por un proveedor de servicios de certificación.

1.5.5. Usuarios finales

Los suscriptores son usuarios finales, personas naturales o jurídicas que tienen capacidad para solicitar y obtener un certificado digital bajo las premisas establecidas en la Declaración de Prácticas de Certificación de cada proveedor de servicios de certificación y las Políticas de Certificados vigentes para cada tipo de certificado de los proveedores. Son usuarios finales: solicitantes, suscriptores y terceros que confían en certificados emitidos por el proveedor.

1.5.6. Solicitante

El solicitante es aquella persona jurídica, pública o privada, nacional o extranjera que cumplan con los requisitos establecidos en las leyes competentes que operan en el país.

1.5.7. Suscriptor

El suscriptor es aquella persona jurídica, pública o privada, nacional o extranjera a quien se ha emitido por parte de la Unidad de Firma Electrónica y se considera suscriptor mientras dicho certificado se encuentre vigente, configurándose este como titular del certificado.

1.5.8. Terceros que confían

Los terceros que confían son las personas o entidades que en forma libre y voluntaria deciden confiar y aceptar un certificado digital emitido por la jerarquía de certificación de El Salvador.

La Unidad de Firma Electrónica de MINEC no asume ningún tipo de responsabilidad ante terceros, que, incluso de buena fe, no hayan verificado convenientemente la vigencia de los certificados.

1.6. Uso de los certificados:

1.6.1. Uso apropiado de los certificados

Los certificados de diferentes tipos emitidos por las AC Raíz y AC Subordinadas bajo esta DPC serán utilizados solamente durante su período de vigencia para dar cumplimiento a las funciones que le son propias y legítimas.

Los certificados deben utilizarse de acuerdo a los fines y especificaciones definidos en las respectivas PC y solamente pueden ser utilizados para los fines contemplados en las PC.

1.6.1.1. Firma de certificados de usuario final

Los certificados de usuario final generados podrán ser firmados a partir de cada una de los PSC y TSA acreditados en El Salvador de acuerdo a sus políticas y declaraciones de prácticas de certificación.

1.6.1.2. Firma de CRL

Los certificados de usuario final generados a partir de un proveedor de servicios de certificación firmarán la lista de certificados revocados CRL.

1.6.2. Usos prohibidos de los certificados

La realización de operaciones no autorizadas según esta DPC, por parte de terceros o suscriptores del servicio, eximirá a la Unidad de Firma Electrónica de cualquier responsabilidad por este uso prohibido, en consecuencia:

- No se permite el uso de los certificados de usuario final para firmar otros certificados o listas de revocación (CRL).
- Está prohibido utilizar los certificados para usos distintos a los estipulados en los numerales correspondientes a: *Uso apropiado de los certificados y límites de uso de los certificados.*
- Se prohíbe el uso de certificados que puedan ocasionar daños personales o medioambientales.
- Se considera prohibida toda acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente DPC.

1.7. Límites de uso de los certificados

Los certificados autoridad de certificación serán utilizados para actuar como Autoridad de Certificación Subordinada de los PSC o TSA, firmando otros certificados de clave pública de entidad final y listas de certificados revocados (CRL).

1.8. Administración de la Declaración de Prácticas de Certificación

La Unidad de Firma Electrónica del MINEC administra la presente Declaración de Prácticas de Certificación, encargada de su elaboración, registro, mantenimiento y actualización.

Los datos de la organización y la persona de contacto disponibles para información al respecto son:

1.8.1. Organización que administra la DPC

MINISTERIO DE ECONOMÍA

UNIDAD DE FIRMA ELECTRÓNICA

ALAMEDA JUAN PABLO II, CALLE GUADALUPE, EDIFICIO C-2 SEGUNDO NIVEL.

CENTRO DE GOBIERNO.

SAN SALVADOR, EL SALVADOR.

1.8.2. Persona de contacto

Para cualquier consulta, diríjanse a:

MINISTERIO DE ECONOMÍA

UNIDAD DE FIRMA ELECTRÓNICA

ALAMEDA JUAN PABLO II, CALLE GUADALUPE, EDIFICIO C-2 SEGUNDO NIVEL.

CENTRO DE GOBIERNO.

SAN SALVADOR, EL SALVADOR.

ING. OSCAR HUMBERTO CRUZ GUARDADO

JEFE DE LA UNIDAD DE FIRMA ELECTRÓNICA

TELÉFONO: +503 2590 5640

EMAIL: FIRMA.ELECTRONICA@ECONOMIA.GOB.SV

1.8.3. Persona que determina la idoneidad e integridad de la DPC

La persona que determina la idoneidad e integridad de la DPC es el titular de la Unidad de Firma Electrónica del Ministerio de Economía.

1.8.4. Procedimientos de emisión de la DPC

La Declaración de Prácticas de Certificación se emite mediante de la Unidad de Firma Electrónica del Ministerio de Economía.

1.9. Definiciones y siglas

1.9.1. Definiciones

En el desarrollo de la presente DPC los términos empleados y sus correspondientes definiciones son los siguientes:

Auditoría: Procedimiento utilizado para comprobar la eficiencia de los controles establecidos a la operación de la Entidad, en la prevención y detección de fraudes o mediante la realización de exámenes a aplicaciones concretas, que garanticen la fiabilidad e integridad de sus actividades.

Autenticación: Proceso electrónico mediante el cual se verifica la identidad de un proveedor de servicios de certificación, solicitante o suscriptor de un certificado emitido como Autoridad de Certificación.

Autoridad de Certificación (AC): Entidad encargada de emitir y revocar certificados digitales utilizados en firma electrónica y cuya clave pública está incluida en éstos.

Autoridad de Registro (AR): Entidad encargada de receptar las solicitudes de certificados, identificar y autenticar la información de los solicitantes de certificados, aprobar o rechazar las solicitudes de certificados, revocar o suspender certificados en determinadas circunstancias, y aprobar o rechazar las solicitudes para renovar o volver a introducir sus solicitudes de certificados.

ARL (Authority Revocation List): Lista de certificados revocados emitida por la AC Raíz que contiene la lista de todos los certificados de AC Subordinada emitidos por la AC Raíz que hayan sido revocados o suspendidos y que aún no hayan expirado.

Cadena de confianza: También conocida como Jerarquía de Confianza, la constituyen las autoridades de certificación relacionadas por la confiabilidad en la emisión de certificados digitales entre diferentes niveles jerárquicos. En el caso salvadoreño serán todos los proveedores de servicios de certificación acreditados por la Unidad de Firma Electrónica.

Normas CEN EN 419 221: Parte de 2-5, según corresponda requisitos de seguridad para módulos criptográficos HSM.

Clave privada: Es la clave, de un par de claves, que es conocida solamente por el usuario o titular del certificado.

Clave pública: Es la clave, de un par de claves, que se conoce públicamente.

CRL (Certificate Revocation List): Lista de certificados que han sido revocados.

CSR (Certificate Signature Request): solicitud de firma de certificado, contiene la información de la petición del certificado.

ETSI: European Telecommunications Standards Institute, Instituto europeo de normas de telecomunicaciones.

ETSI EN 319 411 Part 1: Firma Electrónica e Infraestructuras, Requisitos de política y seguridad para proveedores de servicios de certificación que emiten certificados, Requerimientos Generales.

- sección 6.5.2 de ETSI EN 319 411-1 – Relacionada con módulos criptográficos.

ETSI EN 319 411 Part 2: Firma Electrónica y Infraestructuras, Requisitos de política y seguridad para proveedores de servicios de certificación que emiten certificados, Requerimientos para proveedores de servicios de certificación que emiten certificados digitales.

ETSI EN 319 412-1: Firma Electrónica y Infraestructuras, Perfiles de Certificados, Visión general y estructuras de datos comunes.

FIPS: Federal Information Processing Standard, es un estándar de seguridad para la acreditación de módulos criptográficos.

FIPS 140-2 nivel 3: valida el cumplimiento de su estándar PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, bajo su programa de validación Cryptographic Module Validation Program (CMVP).

HSM (Hardware Security Module): Es un componente o dispositivo criptográfico utilizado para generar, almacenar y proteger claves criptográficas.

ISO: Organización Internacional de Normalización

ISO/IEC 19790 nivel 3: especifica los requerimientos de seguridad para un módulo criptográfico utilizado dentro de un sistema de seguridad que protege información sensible en sistemas informáticos y de telecomunicaciones.

OCSP (Online Certificate Status Protocol): Protocolo de consulta en línea de estado de certificados utilizado para comprobar el estado de un certificado digital en el momento en que es utilizado. Proporciona información actualizada y complementaria del listado de certificados revocados.

OID (Object Identifier): El Identificador de Objetos constituye el valor de una secuencia de componentes variables utilizado para nombrar a casi cualquier tipo de objeto en los certificados digitales, tales como los componentes de los nombres distintivos DN, DPC, PC, etc.

PKCS (Public Key Cryptography Standard): Estándares de criptografía de claves públicas.

PKCS#10: Estándar de criptografía de clave pública utilizado para procesar la petición de un certificado y solicitar la generación de una clave.

PKI (Public Key Infrastructure): Infraestructura de Clave Pública es el conjunto de elementos informáticos (hardware y software), políticas y procedimientos necesarios para brindar servicios de certificación digital.

Política de certificados: Documento que complementa la Declaración de Prácticas de Certificación y que contiene un conjunto de reglas que norman las condiciones de uso y los procedimientos seguidos por la Unidad de Firma Electrónica de MINEC para la emisión de certificados, determinando la aplicabilidad de un certificado de Autoridad de Certificación.

RFC (Request for comments): Publicaciones de *Internet Engineering Task Force* que en forma de memorandos contienen protocolos y procedimientos para regular el funcionamiento de Internet.

Sellado de tiempo: Anotación firmada electrónicamente y agregada a un mensaje de datos mediante procedimientos criptográficos en la que consta como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación, basándose en la RFC 3161 Internet X.*509 Public Key Infrastructure Time-Stamp Protocol (TSP)*.

X.509: Estándar desarrollado por la UIT-T para infraestructuras de clave pública que especifica entre otros temas, los formatos estándar para certificados de claves públicas y para la implementación de listas de certificados revocados.

1.9.2. Siglas

AR	autoridad de registro (Registration Authority)
ARL	Lista de Revocación de Autoridades (Authority Revocation List)
C	Nombre País (CountryName)
CA	Autoridad de Certificación (Certification Authority)
CN	Nombre Común (CommonName)
CPS	Declaración de Prácticas de Certificación (Certificate Practice Statement)
CRL	(Lista de Certificados Revocados (Certificate Revocation List)
DUI	Documento Unico de Identidad (National ID Card in El Salvador)
CSR	Solicitud de firma de certificado (Certificate Signing Request)
FC	Firma Centralizada (Remote Digital Signature)
HSM	Dispositivo Módulo de Seguridad (Hardware Security Module)
ISO	Organización Internacional de Estandarización (International Organization for Standardization)
L	Localidad (LocalityName)

MINEC	Ministerio de Economía (Ministry of Economic)
NIT	Número de Identificación Tributaria (Salvadorian VAT Number)
NRC	Número de Registro de Contribuyente
O	Nombre de Organización (OrganizationName)
OCSP	Protocolo Online de Estado del Certificado (Online Certificate Status Protocol)
OID	Identificador de Objetos (Object IDentifier)
OU	Nombre de Unidad Organizativa (OrganizationalUnitName)
PAS	Pasaporte (Passport)
PKCS	Estándar de Clave Pública (Public-Key Cryptography Standard)
PKI	Infraestructura de Clave Pública (Public Key Infrastructure)
PSC	Proveedores de Servicios de Certificación (Certification Services Provider)
RA	Autoridad de Registro (Registration Authority)
SFC	Servidor de Firma Centralizada (Centralized Signature Server)
SHA	Algoritmo Seguro de Resumen (Secure Hash Algorithm)
ST	Nombre de Provincia o Estado (STateOrProvinceName)
TSA	Autoridad de Sellado de Tiempo (Time-Stamping Authority)
UO	Unidades Organizativas (Organizational Units)
UTC	Tiempo Universal Coordinado (Universal Time Coordinated)
V	Versión (Version)
VA	Autoridad de Validación (Validation Authority)
VAT	Impuesto al Valor Agregado (Value Added Tax)

2 Publicación de la Información y Responsabilidades de los Repositorios

La responsabilidad de la publicación de la presente DPC, así como los documentos de Políticas de Certificado y las ARL, le corresponde a la Unidad de Firma Electrónica del Ministerio de Economía. La Declaración de Prácticas de Certificación y las Políticas de Certificados son documentos públicos que se encuentran disponibles en la página web. Las modificaciones a los documentos mencionados, que fueren aprobadas de acuerdo al procedimiento establecido se harán públicas de forma inmediata.

2.1. Repositorios

La documentación mencionada en el párrafo anterior se encuentra disponible en la página web de la Unidad de Firma Electrónica. La Declaración de Prácticas de Certificación (DPC), medios de publicación, frecuencia de publicación y el control de acceso al directorio de certificados, estará disponible para suscriptores y usuarios vía electrónica en la página web http://normativa.firmaelectronica.economia.gob.sv/dpc/. En el repositorio de documentos se podrá consultar esta información.

2.2. La publicación de la DPC

La Declaración de Prácticas de Certificación estará disponible a través del portal web indicado en el apartado anterior, cualquier cambio o modificación en la DPC generará una nueva versión, debiendo publicarse dicho cambio, además de guardar y custodiar la versión anterior, toda vez que al amparo de esta última pudiesen haberse originado derechos y obligaciones para los suscriptores y usuarios de las mismas.

2.3. Frecuencia de la publicación

La Unidad de Firma Electrónica gestiona y mantiene actualizado el repositorio conforme a la siguiente frecuencia:

- Directorio de certificados digitales emitidos Proveedores de Servicios de Certificación: Actualizado cada vez que se emite un nuevo certificado digital.
- Listas de certificados digitales revocados: Actualizado cada vez que se revoca un certificado digital de PSC y TSA o con la emisión de una nueva ARL.
- Política de Certificación (PC): Actualizado cada vez que se emita una nueva versión de la misma.
- Declaración de Prácticas de Certificación (DPC): Actualizado cada vez que se emita una nueva versión.

- Política de Seguridad: Actualizado cada vez que la emite una nueva versión.
- La información del directorio de certificados emitidos por Proveedores de Servicios de Certificación y Listas de certificados revocados: Actualizado cada vez que se emita o se revoque un certificado de Proveedores de Servicios de Certificación

2.4. Control de acceso a los repositorios

El acceso a la consulta del directorio de certificados y la ARL es libre, al igual que en todos los procesos de la vida de los certificados, sin embargo, se dispone de la seguridad y controles para garantizar que la información del directorio no sea alterada. Es responsabilidad de la Unidad de Firma electrónica establecer controles que impidan a personas no autorizadas manipular la información contenida en los repositorios, así como la adopción de las medidas de seguridad necesarias para garantizar la integridad, autenticidad y disponibilidad de dicha información.

3 Identificación y Autenticación

En esta sección se describen los procedimientos específicos y criterios aplicados por la Autoridad de Certificación Raíz al momento de autenticar la identidad del proveedor de servicios de certificación para la aprobación de la emisión del certificado correspondiente.

3.1. Nombres

De acuerdo a la política de certificación se establece la necesidad de la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado, para vincular la clave pública con su identidad.

3.1.1. Tipos de nombres

Todos los certificados de PSC y TSA tienen una sección llamada SubjectDN cuyo objetivo es permitir identificar al suscriptor o titular del certificado, incluyendo un Distinguished Name (DN) caracterizado por un conjunto de atributos que conforman un nombre diferenciado, único e inequívoco para cada proveedor de servicios de certificación.

Atributo	Nombre en Inglés	Nombre	Descripción
C	Country	País	*Abreviatura del país del proveedor de servicio de certificación*
L	Locality	Ciudad	*Nombre de la LOCALIDAD del domicilio del PSC o TSA*
OU	Organizational Unit	Unidad organizativa	*Nombre de la Unidad Organizativa del PSC o TSA*
O	Organization	Organización	*Nombre de la Organización del PSC o TSA*
CN	Common Name	Nombre común	*Nombres y apellidos completos del suscriptor*
organizationId entifier	Organization Identifier	Identificador de la Organización	*NIT del proveedor de servicio de certificación*

**En el caso de El Salvador la localidad será municipio, departamento. Para el caso de extranjeros se revisará según sea el caso.*

Para incluir una dirección de correo electrónico (e-mail) de contacto del proveedor de servicio de certificación, dicha información se debe colocar en el campo rfc822Name de la extensión

"SubjectAltName" tal como se indica en la ETSI EN 319 412-2 V2.1.1 (2016-02), de acuerdo con lo indicado en los requerimientos genéricos y en cumplimiento con el estándar IETF TFC 5280.

3.1.2. Necesidad de que los nombres sean significativos

El campo SubjectDN de todos los certificados digitales de la jerarquía de certificación debe permitir determinar sin ambigüedad la identidad del suscriptor, necesarios para la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado.

3.1.3. Anonimato o seudónimos en los nombres

La Unidad de Firma Electrónica no admite anónimos ni seudónimos para identificar el nombre de proveedor de servicios de certificación.

3.1.4. Reglas para interpretar las diversas formas de nombres

Las reglas para interpretar los formatos de nombre *IssuerDN* y siguen lo señalado por la familia de estándares ISO/IEC 9594 (recomendación X.500). Así, la estructura de un DN *(DistinguishedName)* se define en el estándar ISO/IEC 9594-2 (recomendación ITU-T X.501), que es construida con los atributos definidos en el estándar ISO/IEC 9594-6 (recomendación ITU-T X.520). Los numerales 4.1.2.4 y 4.1.2.6 de la RFC 5280, indican el conjunto de atributos obligatorios y opcionales que deben contener los campos *IssuerDN* y *SubjectDN*.

3.1.5. Unicidad de los nombres

Los nombres distintivos en los certificados de proveedores de servicios de certificación son únicos para cada autoridad de certificación subordinada. En cualquier caso, la Unidad de Firma Electrónica de MINEC utiliza mecanismos para evitar conflictos de nombres.

3.1.6. Validación inicial de la identidad

La Unidad de Firma Electrónica valida el derecho que posee un solicitante para gestionar un certificado de autoridad de certificación. La solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado, con las atribuciones y los poderes de representación correspondientes.

3.1.7. Método para probar la posesión de la clave privada

Los proveedores de servicios de certificación deben generar su propio par de claves, deben demostrar la posesión de su clave privada mediante el envío de un mensaje de prueba de posesión de clave privada, conforme a lo estipulado en el RFC4210, como por ejemplo un Certificate Signing Request (CSR) en formato PKCS#10, según lo estipulado en el RFC2986.

3.1.8. Autenticación de la identidad de PSC o TSA

El solicitante, para demostrar su identidad, debe proporcionar información suficiente para acreditarse como proveedor de servicios de certificación, conforme a la normativa aplicable.
La información suministrada por el solicitante a través del formulario a la Autoridad de Registro, junto con la documentación de soporte, será revisada por el personal de la Unidad de Firma Electrónica encargado de acreditar a los proveedores de servicios de certificación de acuerdo a los procedimientos internos definidos por la Unidad de Firma Electrónica de MINEC.

3.1.9. Información de solicitante no verificada

En la solicitud del certificado de autoridad de certificación el solicitante debe proporcionar documentos y datos personales que lo identifiquen absolutamente, toda la información será verificada aún si no hace parte de la información incluida en el certificado digital del PSC o TSA. Se debe dejar constancia de la información no verificada.

3.1.10. Validación de la autoridad

La Unidad de Firma Electrónica debe validar el derecho que posee un solicitante para gestionar un certificado de autoridad de certificación. La solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado y con las atribuciones y los poderes de representación correspondientes.

3.1.11. Criterios para la interoperación

La jerarquía de la autoridad de certificación raíz de El Salvador debe operar independientemente de otras PKI; sin embargo, se debe garantizar la interoperabilidad con las PKI que satisfagan los requisitos técnicos y jurídicos en conformidad con la legislación y normativa nacional.

3.1.12. Identificación y autenticación para solicitudes de revocación

El procedimiento para identificación y autenticación para generar la solicitud de revocación de un certificado de autoridad de certificación mediante un formulario.

4 Requisitos Operacionales para el Ciclo de Vida de los Certificados

El ciclo de vida de los certificados digitales para los proveedores de servicios de certificación, bajo la jerarquía de CA raíz en El Salvador contempla: emisión, expiración, revocación y renovación de certificados digitales.

La Unidad de Firma Electrónica procesará las solicitudes de emisión de certificados digitales para los Proveedores de Servicios de Certificación que hayan sido acreditados. La Unidad de Firma Electrónica aceptará únicamente solicitudes de emisión y pedidos de revocación de certificados digitales a través del representante legal de la entidad, o apoderado debidamente autorizado por ésta.

4.1. Solicitud de certificado

El procedimiento para solicitud de un certificado digital se describe detalladamente en la correspondiente Política de Certificados, sin perjuicio de la información requerida obligatoriamente.

4.1.1. Proceso de registro y responsabilidades

El solicitante de un certificado digital debe llenar el correspondiente formulario con toda la información requerida en el mismo. No toda la información requerida en el proceso de registro aparecerá en el certificado y será conservada de manera confidencial por la Autoridad de Certificación.

La Unidad de Firma Electrónica en función de sus actividades, garantizará el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de ese carácter, así como su correspondiente protección.

4.1.2. Proceso de solicitud del certificado

En el proceso de solicitud del certificado el solicitante debe suministrar diversos datos que lo identifican plenamente, de acuerdo a las previsiones de la normativa aplicable. La información proporcionada en la solicitud del certificado digital es verificada con la finalidad de determinar su autenticidad.

4.1.3. Procesamiento de las solicitudes

Las solicitudes de emisión de un certificado digital serán direccionadas por la Autoridad de Registro a la Autoridad de Certificación para la verificación y autenticación de los datos registrados en la solicitud.
El tiempo para aprobar una solicitud está establecido por la Ley de Firma Electrónica de El Salvador y su regulación.

4.1.4. Procesamiento de identificación y autenticación

La Autoridad de Registro deberá comprobar y validar la información y los documentos que son requeridos para solicitar los certificados digitales.

La Unidad de Firma Electrónica mantendrán un archivo con la información que respalde cada solicitud de inscripción realizada para la emisión de los certificados de PSC o TSA, por un periodo de mínimo diez (10) años contados a partir de la expiración del certificado.

4.1.5. Aprobación o archivo de la solicitud de certificados

Si el proceso de verificación y validación de la documentación e información entregada por el solicitante resulta exitosa, la Unidad de Firma Electrónica aprobará dicha solicitud y notificará al proveedor para continuar con el proceso de acreditación y emisión del certificado de autoridad de certificación.

Se archivarán, notificando la causa, las solicitudes que no cumplan con los requerimientos, información y documentación solicitada por la Unidad de Firma Electrónica.

4.2. Emisión de certificados

La emisión del certificado se produce el momento en que la Autoridad de Registro ha comprobado fehacientemente la validez de la solicitud realizada. El mecanismo para realizar esta validación está descrito en la Política de Certificación correspondiente.

Le corresponde a la AR notificar al suscriptor de un certificado cuando se ha producido la emisión del mismo. En todo momento el usuario suscriptor es el único que tiene acceso a la clave privada del certificado digital.

4.2.1. Acciones de la AC durante la emisión del certificado

La Unidad de Firma Electrónica emitirá un certificado digital de proveedores de servicio de certificación, si recibe una solicitud de emisión acompañada de un mensaje de prueba de posesión de clave privada, conforme a lo estipulado en el RFC4210, como una petición de firma de certificado (CSR) válido en formato PKCS#10, según lo indicado en la solicitud de certificado digital.

4.2.2. Notificación al suscriptor por parte de la AC de la emisión del certificado

La notificación de la emisión y entrega puede realizarse mediante medios telemáticos a través del envío del certificado al proveedor de servicio de certificación.

4.3. Aceptación del certificado

4.3.1. Aceptación del certificado por el solicitante

La aceptación del certificado digital se da en el momento en el que titular del certificado expresa la aceptación de los términos y condiciones contenidos en la acreditación como PSC o TSA.

4.3.2. Publicación del certificado

Emitido el certificado de PSC o TSA por parte de la Unidad de Firma Electrónica, se procede a su publicación en el directorio de certificados. La clave pública del certificado es publicada en el correspondiente repositorio de lista de proveedores de servicios de certificación.

4.4. Par de claves y uso del certificado

4.4.1. Uso de la clave privada y del certificado por parte del suscriptor

El suscriptor podrá utilizar la clave privada y el certificado exclusivamente para los usos autorizados en esta política de certificación, luego de que el suscriptor haya aceptado los términos y condiciones de la misma.

4.4.2. Uso de la clave pública y del certificado por los terceros que confían

Los terceros que confían, deben usar la clave pública contenida en el certificado para realizar las validaciones indicadas únicamente en las extensiones *KeyUsage (KU)* del certificado o en la presente política de Certificación

Los usuarios que confían deben verificar el estado del certificado utilizando los mecanismos establecidos en la presente DPC y en la PC correspondiente.

4.4.3. Renovación del certificado

La renovación del certificado se produce cuando éste va a expirar, para esto el suscriptor deberá realizar el mismo procedimiento utilizado para solicitar un certificado de PSC o TSA, sin embargo, datos de arquitectura y demás presentados para la acreditación servirán para el nuevo proceso de generación del par de claves.

4.5. Renovación de certificados con cambio de clave

No Aplica.

4.6. Modificación de certificados

4.6.1. Circunstancias para la modificación de un certificado

El certificado no puede ser modificado. Todas las modificaciones de certificados realizadas se tratarán como una nueva emisión de certificado.

4.7. Revocación de certificados

La revocación de los certificados son mecanismos que se utilizan cuando existe la pérdida de fiabilidad de los mismos, ocasionando el cese de su operatividad e impidiendo su uso legítimo.

La revocación de un certificado tiene como principal efecto la terminación inmediata y anticipada del periodo de validez del mismo.

Los certificados revocados no podrán bajo ninguna circunstancia volver al estado activo.

La revocación de un certificado implica su publicación en la Lista de Certificados Revocados de Autoridad de Certificación (ARL) de acceso público.

4.7.1. Circunstancias para la revocación

Los certificados emitidos por la Autoridad de Certificación Raíz de El Salvador serán revocados bajo las siguientes circunstancias:

- Por exposición, puesta en peligro, uso indebido o compromiso de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Cuando la información contenida en el certificado digital no resulte correcta, pueda ser fraudulenta.
- Por el cese en la actividad como proveedor de servicios de certificación.

4.7.2. Obligación de consulta de información de revocación o suspensión de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Autoridades más reciente emitida por la Autoridad de Certificación Raíz.

Las Listas de Revocación de Autoridades se publican en el Depósito de la Autoridad de Certificación Raíz, así como en las siguientes direcciones web:

- http://crl1.firmaelectronica.economia.gob.sv/crl/arl_sv.crl
- http://crl2.firmaelectronica.economia.gob.sv/crl/arl_sv.crl

4.7.3. Frecuencia de emisión de listas de revocación de autoridades (ARL)

La Lista de Revocación de Autoridades se emite por la Autoridad de Certificación Raíz al menos cada 6 meses.

4.7.4. Disponibilidad de servicios de comprobación en línea de estado de certificados

Los terceros que confían en los certificados podrán consultar el estado de los mismos en el repositorio de la Autoridad de Certificación Raíz, que se encuentra disponible 24 horas de los 7 días de la semana en la web:

- https://normativa.firmaelectronica.economia.gob.sv/dpc/

Para comprobar la última ARL se pueden consultar las siguientes direcciones web:

- http://crl1.firmaelectronica.economia.gob.sv/crl/arl_sv.crl
- http://crl2.firmaelectronica.economia.gob.sv/crl/arl_sv.crl

4.7.5. Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados ante de confiar en los mismos.

4.8. Finalización de la suscripción

La acreditación como PSC o TSA es indefinida, pero la validez del certificado como autoridad de certificación va de acuerdo a la vigencia del certificado.

5 Controles de Seguridad Física, Instalaciones y Gestión y Operacionales

Los aspectos referentes a los controles de seguridad física, de las instalaciones, de personal, auditoría y operacionales, definidos para trabajar en un ambiente fiable y seguro, se encuentran especificados en la presente Declaración de Prácticas de Certificación de la Autoridad de Certificación Raíz de El Salvador.

5.1. Controles de seguridad física

5.1.1. Ubicación y seguridad ambiental

La infraestructura de clave pública está aislada físicamente del resto de sistemas del Ministerio de Economía.

Las instalaciones donde se resguarda o efectúa el procesamiento de información sensible cuenta con las siguientes características físicas:

- Puertas sólidas para impedir y prevenir el acceso a personal no autorizado.
- Personal de seguridad que sólo permita el ingreso a personas autorizadas.
- Los visitantes deben ser escoltados en todo momento dentro de las áreas restringidas de la Unidad de Firma Electrónica.
- Medidas de prevención ante desastres naturales (Terremoto, entre otros) y ante desastres accidentales creados por el hombre (incendios, explosiones, disturbios civiles).
- Zonas de alta seguridad con activos críticos restringidas con acceso biométrico.
- Instalaciones físicas con al menos dos ambientes separados:
    - Área Operacional: Contiene los equipos y servidores computacionales necesarios para la operación del PSC o TSA.
    - Área Restringida: Contiene la información confidencial y crítica. Por ejemplo, el módulo criptográfico que contiene las claves privadas.
- Documentación que contiene información sensible de texto se almacena en contenedores seguros

5.1.2. Gestión del acceso físico

La infraestructura de la jerarquía raíz de El Salvador está físicamente separada de cualquier otro sistema y el acceso cuenta con un sistema de control de acceso físico de 3 niveles que disponen de los siguientes mecanismos de control:

- Sistema de video seguridad que incluye video vigilancia y grabación con sistema multi-cámara para el monitoreo, grabación, búsqueda y reproducción con múltiples cámaras para brindar

seguridad a áreas de acceso principales, periferia y monitoreo de actividades en las instalaciones.

- Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro que cuenta con puertas de seguridad y control de acceso biométrico y/o contraseña de acceso.

5.1.3. Energía y aire acondicionado

5.1.3.1. Energía

Se cuenta con un grupo electrógeno capaz de soportar y suministrar la energía necesaria para el funcionamiento normal de los sistemas y equipos en caso de ausencia de suministro de energía eléctrica de la red pública.

Los tableros eléctricos de distribución de energía normal cuentan con un sistema de barras de cobre correctamente dimensionadas y breakers de protección y UPS. Cuenta con tableros de bypass, uno para cada equipo de protección UPS y tableros de distribución de red regulada.

5.1.3.2. Aire acondicionado

Las instalaciones donde está la infraestructura PKI poseen un sistema de climatización con sistemas de precisión de alto rendimiento, e incluyen equipo electrónico sensible, preciso, fiable en el control de la temperatura ambiente, la humedad y el flujo de aire para un rendimiento óptimo, con el objetivo de mantener una temperatura controlada de acuerdo a los requerimientos técnicos.

5.1.4. Exposición al agua

Las instalaciones cuentan con sistemas de piso de acceso elevado, con paneles rellenos con inyección de cemento, laminado y fórmica de alta precisión y propiedades anti fuego y antiestática.

Cuenta con controles de humedad y temperatura, sistemas de drenaje y piso elevado, para evitar el riesgo de exposición al agua. El sistema de detección de fugas de agua (WLD) se ha instalado en las instalaciones para garantizar la seguridad en caso de una fuga de agua.

5.1.4.1. Prevención y protección de incendios

El sistema de detección y extinción de incendios automática cumple con las normas UL S2203 Y FM 3023436 y posee un mecanismo de control vía software con tecnología de comunicación

bidireccional punto a punto con capacidad de respuesta de ¼ de segundo en la detección de incendios.

5.1.5. Seguridad de los servidores de almacenamiento

Se dispone de copia fuera de del sitio principal donde se encuentra instalada la jerarquía raíz en lugares cercanos a las instalaciones del sitio principal.

5.2. Controles de procedimientos

5.2.1. Roles de administración y operación

Existen dos tipos de roles para la administración y operación de los componentes de la PKI, según el mecanismo de creación y sus acciones permitidas:

- Roles estáticos fijados en cada componente con las siguientes características: no se pueden crear nuevos roles estáticos, eliminar alguno de los existentes o modificar sus acciones permitidas.

- Los roles establecidos para la administración y operación de la jerarquía raíz en todos o parte de los componentes que la integran, según lo definido en las normas CEN EN 419 221, partes 2 a 5, según proceda, son los siguientes:

  - **Administrador de Seguridad:** tiene la responsabilidad de administrar la implementación de políticas y prácticas de seguridad, la operación de recuperación de datos y las operaciones de archivo (backup) y recuperación de claves.

  - **Administrador de Sistema**: está autorizado para instalar, configurar y mantener los equipos con acceso controlado a la información de seguridad y la administración de las BD del equipo.

  - **Operador de Sistema:** responsable de operar los sistemas y la operación de archivo (backup) manual de datos. Además, puede realizar la monitorización y administración del hardware y software del equipo y de administración de sus servicios.

  - **Administrador de CA**: responsable de la instalación y configuración de los equipos y material criptográfico, o con la realización de alguna función que implique la activación

de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.

- **Operador de CA**: encargado de la de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la CA.

- **Auditor**: encargado de la auditoría de las operaciones y revisión de los logs y procesos de la infraestructura de clave pública.

- **Operador de Registro**: encargado de administrar el ciclo de vida de los certificados: generación, renovación y reemisión de certificados, así como revocación, suspensión y rehabilitación de los certificados.

5.2.2. Requisitos de identificación y autenticación para cada rol

El acceso a la operación y administración de todos los componentes de la PKI requiere de la autenticación múltiple para ejecutar las tareas sensibles permitidas de acuerdo al rol asignado.

5.3. Controles del personal

5.3.1. Requisitos

Los requisitos de calificación que cumple el personal que desempeña las distintas actividades en el proceso de administración de la PKI son los siguientes:

- Título profesional o experiencia equivalente.
- Conocimiento y experiencia en la materia de infraestructura de clave pública.
- Capacitación específica para la función desempeñada.

5.3.2. Verificación de antecedentes

El personal que desempeña las funciones operativas en el funcionamiento de la Unidad de Firma Electrónica deberá demostrar documentadamente su formación académica, su experiencia profesional y sus conocimientos y experiencia en el desarrollo de las funciones técnicas encomendadas. La Unidad de Firma Electrónica realizará una verificación de antecedentes para verificar la información mencionada.

- No podrá prestar estos servicios, el personal que haya tenido antecedentes de negligencia o incumplimiento de funciones relacionados a infraestructura de clave pública PKI previamente.
- No se permitirá que ningún personal con antecedentes penales realice funciones operativas en CA Raíz.

5.3.3. Capacitación y entrenamiento

Adicionalmente al conocimiento de la normativa emitida por la Unidad de Firma Electrónica, los conocimientos de que dispone el personal se ajustan, pero no se limitan a:

- Conceptos acerca de PKI.
- Servicios prestados por la Unidad de Firma Electrónica
- Aspectos legales relativos a la provisión de servicios de certificación.
- Seguridades física y lógica de las tareas y roles.
- Procedimientos para la operación, administración y mantenimiento de acuerdo a cada rol específico.
- Gestión de incidencias.
- Procedimientos para la operación en caso de desastres.

Se debe determinar el momento oportuno para impartir capacitación al personal involucrado en las operaciones. Se debe impartir al menos una capacitación al inicio de funciones (inducción) y una actualización anual. La inducción y actualizaciones deben contener al menos los siguientes aspectos:

- Uso y operación del hardware y software empleado.
- Aspectos relevantes de la Política de Certificación, Declaración de Prácticas de Certificación, Política de Seguridad y otra documentación que comprenda sus funciones.
- Marco regulatorio de la provisión de los servicios de certificación.
- Procedimientos en caso de contingencias.
- Procedimientos de operación y administración para cada rol específico.
- Procedimientos de seguridad para cada rol específico.
- Plan de Continuidad del Negocio y Recuperación ante desastres.

5.3.4. Rotación de roles

Para garantizar la adecuada operación de la PKI en procesos operativos se podrá realizar la rotación de funciones entre los diferentes roles asignados con intervalos y secuencias de rotación previamente definidos, no así para los roles de administración de la infraestructura PKI.

5.3.5. Sanciones en caso de acciones no autorizadas

Se dispone de un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.

5.3.6. Documentación suministrada al personal

Toda la documentación relativa al desenvolvimiento de las tareas y procesos que desarrolla Unidad de Firma Electrónica será entregada al personal durante su formación inicial para su conocimiento y aplicación.

5.3.7. Procedimientos de registro de auditoria – Controles de auditoría

Los equipos de los componentes de la PKI generarán eventos de auditoría que serán almacenados en las correspondientes bases de datos y en ficheros locales.

5.3.8. Tipos de eventos registrados y auditados

Los siguientes son los eventos del ciclo de vida del certificado que serán registrados y auditados:

- Los accesos a los componentes de la PKI por los administradores y operadores.
- Las solicitudes de emisión, renovación, suspensión, rehabilitación y revocación de certificados y el administrador u operador que ejecuta la acción.
- La generación o renovación de certificados.
- La generación o revocación de claves.
- La actualización de la ARL y su publicación.
- Intentos de modificar o borrar la información de los titulares de certificados.
- Back up, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal.

5.3.9. Frecuencia de procesamiento de los registros de auditoría

La frecuencia para realizar el análisis y procesamiento de los registros de auditoría será determinada por la Unidad de Firma Electrónica del Ministerio de Economía.

5.3.10. Período de resguardo de los registros de auditoría

Los registros de auditoría se conservarán durante mínimo diez (10) años a partir de su generación.

5.3.11. Protección de los registros de auditoría

Únicamente la o las personas que desempeñen la función de Auditor tiene acceso a los registros auditados. Ningún operador tiene permisos para modificar o borrar los registros.

5.3.12. Procedimiento de respaldo de los registros de auditoría

La Unidad de Firma Electrónica genera copias locales y en sitio remoto periódicamente de los registros de auditoría. Los archivos de respaldo de las auditorías se guardan en el centro de datos de la PKI.

5.3.13. Análisis de vulnerabilidades

La infraestructura de clave pública dispone de una herramienta que identifica ataques potenciales para vulnerar la seguridad del sistema. La presentación del resultado del análisis de vulnerabilidades implica corregir las vulnerabilidades detectadas y la emisión de los correspondientes informes, de acuerdo a la política de seguridad del Ministerio de Economía.

5.4. Almacenamiento y archivo de la información

5.4.1. Tipo de información a resguardar

Se guardan archivos relacionados con el ciclo de vida de los certificados, entre los que se encuentran:

- Las solicitudes de certificados.
- El documento de acreditación como proveedores de servicios de certificación.
- Los datos suministrados y la información de soporte entregada.
- Cualquier otra que ordene la normativa aplicable.

5.4.2. Período de resguardo de la información

En la Unidad de Firma Electrónica los datos acerca del ciclo de vida de los certificados emitidos son almacenados por un período mínimo de diez (10) años contados a partir de la fecha de expiración del certificado.

5.4.3. Sistemas de almacenamiento

Toda la información relacionada con la auditoría en la Unidad de Firma Electrónica es interna y archivada en sus propias instalaciones.

5.4.4. Procedimiento para obtener y verificar la información archivada

Se podrá determinar un procedimiento para obtener y verificar la información archivada manteniendo dos copias de los archivos de datos bajo administración y control de dos personas asignadas al efecto, para de esta manera compararlas para asegurar que las copias sean exactas.

De forma automática se realizan comprobaciones acerca de la integridad de los backups, el tiempo de su generación, y se crea una incidencia en el caso de error o comportamientos imprevistos.

5.5. Compromiso ante incidentes y recuperación de desastres

5.5.1. Procedimientos para administrar incidentes

En caso de que se produjese un incidente que implique la indisponibilidad de los servicios de certificación de la Unidad de Firma Electrónica se procederá a la ejecución del Plan de Continuación del Servicio, el mismo que garantiza que los servicios considerados como críticos por su requerimiento de disponibilidad estén disponibles en menos de veinticuatro (24) horas.

5.5.2. Procedimientos ante compromiso de la clave privada de la AC Raíz

En el supuesto de revocación del certificado de la AC si la clave privada ha sido comprometida, se revocará el certificado, se suspenderá el funcionamiento de la entidad y se procederá a generar una nueva entidad con un nuevo par de claves. El certificado revocado permanecerá accesible en el repositorio de jerarquía raíz de El Salvador con el objeto de permitir la verificación de los certificados emitidos durante su período de funcionamiento.

5.5.3. Capacidad de continuidad del negocio ante un desastre

La Unidad de Firma electrónica garantiza su capacidad para asegurar la continuidad de sus operaciones si se produjera un desastre natural, como un terremoto que destruya las instalaciones, o desastre de cualquier tipo que comprometa su funcionamiento. Una infraestructura redundante existe para garantizar las operaciones.

5.5.4. Medidas para la corrección de vulnerabilidades detectadas

Los servicios de las interfaces web de administración y operación de todos los componentes de la infraestructura PKI y de la interfaz web de usuarios de la AR aplican filtros para impedir que puedan contener código intruso, que pudiese producir, por ejemplo, para vulnerar la base de datos. Las actualizaciones de software en los componentes de la infraestructura PKI vienen firmados para evitar que se introduzca código malicioso dentro de los entornos de producción.

Los servicios de las interfaces web de administración y operación de todos los componentes de PKI y de la interfaz web de usuarios de la AR aplican filtros a todas las páginas que puedan recibir parámetros a través del método GET, incluidos en la URL, para impedir que puedan contener código intruso, que pudiese producir, por ejemplo, cualquier ataque de inyección SQL.

5.5.5. Terminación o disolución de las autoridades de certificación y de registro

Las causas que pueden producir el cese de la actividad de la jerarquía raíz de El Salvador son:

- Compromiso de la clave privada de la AC.
- Mandato legal.

En el supuesto no consentido y muy remoto de disolución de la Unidad de Firma Electrónica el procedimiento a seguir será determinado en el instrumento que acuerde la disolución y debe considerar al menos:

- Todos los suscriptores de PSC o TSA serán notificados de la cesación por correo electrónico.
- Todos los certificados emitidos por la Autoridad de Certificación a las CA subordinadas se revocarán a más tardar en el momento del cese (la ARL emitida debe ser válida al menos hasta 30 días después de que caduque el último certificado emitido por la CA).
- Se archivarán todas las pruebas de identidad, certificado, validación, revocación, política, prácticas y datos de auditoría de CA actuales y conservados.

6 Controles de Seguridad Técnica

La Infraestructura de Clave Pública PKI Raíz de MINEC utiliza productos fiables, que cumplen las normas y certificaciones internacionales sobre la materia, se encuentran protegidos contra toda alteración y de esta manera garantizan la seguridad técnica y criptográfica de los procesos de certificación.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves se genera en módulos de hardware criptográficos que cumplen los requisitos establecidos como Autoridad de Certificación:

- Los módulos criptográficos deben encontrarse certificados conforme a Common Criteria, perfiles de protección descritos en las normas CEN EN 419 221, partes 2 a 5, según proceda[1]; o según el estándar ISO/IEC 19790 nivel 3, como mínimo, o el estándar FIPS 140-2 nivel 3, como mínimo.

Asimismo, las características de los claves de los certificados que conforman la jerarquía tendrán las siguientes características:

Nivel de la jerarquía PKI	Longitud de la clave	Duración máxima
Autoridad de Certificación Raíz	4.096 bits	25 años
Autoridad de Certificación Subordinada	4.096 bits	15 años
- Certificados de entidad final	2.048 bits	Hasta 5 años

6.1.2. Claves de la AC

El par de claves de la AC Raíz y la AC Subordinada se genera de acuerdo con el procedimiento de Ceremonia de Generación de claves desarrollada por la institución.

[1] Cfr. sección 6.5.2 de ETSI EN 319 411-1.

El proceso de generación de claves de la AC raíz de El Salvador fue realizado por personal autorizado según los roles de confianza utilizando un HSM de acuerdo a lo descrito en el numeral 6.1.1 del presente documento.

La AC Raíz permanece apagada y solo es utilizada para la emisión de ARL con un periodo de validez de seis (6) meses o cada que se genere un certificado de AC subordinada, en todo momento este elemento no tiene conexión a red.

6.1.3. Claves del suscriptor

La Unidad de Firma Electrónica debe implementar controles que aseguren la confidencialidad y seguridad en la entrega de la clave privada. La prueba de posesión de la clave privada se realiza según lo indicado en el numeral 6.1.4 y 6.1.5 del presente documento.

6.1.4. Entrega de la clave privada al suscriptor

El par de claves se genera en módulos de hardware criptográficos que cumplen los requisitos establecidos como Autoridad de Certificación:

- Los módulos criptográficos deben encontrarse certificados conforme a Common Criteria, perfiles de protección descritos en las normas CEN EN 419 221, partes 2 a 5, según proceda[2]; o según el estándar ISO/IEC 19790 nivel 3, como mínimo, o el estándar FIPS 140-2 nivel 3[3], como mínimo.

6.1.5. Entrega de la clave pública al suscriptor

El PSC o TSA es quien genera su propio par de claves, la clave pública correspondiente debe ser remitida mediante un mensaje de prueba de posesión de clave privada, conforme a lo estipulado en el RFC4210, como una petición (Certificate Signing Request - CSR) en formato PKCS#10, según lo estipulado en el RFC 2986.

6.1.6. Tamaño de las claves

El tamaño de las claves de certificados de proveedores de servicios de certificación es de 4096 bits.

[2] Cfr. sección 6.5.2 de ETSI EN 319 411-1.
[3] FIPS valida el cumplimiento de su estándar PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, bajo su programa de validación Cryptographic Module Validation Program (CMVP).

Nivel de la jerarquía PKI	Algoritmo de Firma	Tamaño de claves RSA
CA ROOT El Salvador	sha512WithRSAEncryption	4096 bits
CA Subordinada PSC o TSA	sha512WithRSAEncryption	4096 bits

La clave pública de la AC Raíz y de la AC Subordinada está codificada de acuerdo con RFC 5280. El algoritmo de generación de claves es sha512withRSAEncryption.

La clave pública de los certificados emitidos por la jerarquía raíz de El Salvador está codificada de acuerdo con RFC 5280. El algoritmo de generación de claves es sha512withRSAEncryption.

El tamaño de las claves de certificados de entidad final es de 2048 bits.

Nivel de la jerarquía PKI	Algoritmo de Firma	Tamaño de claves RSA
Certificados de Entidad Final	Sha256WithRSAEncryption	2048 bits

El algoritmo de generación de claves de los certificados de entidad final es sha256withRSAEncryption.

6.2. Protección de clave privada

6.2.1. Controles y estándares para los módulos criptográficos

Los módulos utilizados para la creación de las claves a utilizar por las autoridades de certificación disponen de un nivel de seguridad que garantiza su funcionalidad y seguridad, mismos que se encuentran certificados de acuerdo a lo establecido en el numeral **6.1.4 Entrega de clave privada al suscriptor.**

6.2.2. Control multipersona sobre la clave privada

Los proveedores de servicios de certificación deben generar sus claves de tal manera que se proteja su acceso mediante control multipersonal. De un conjunto de "m" personas autorizadas, se debe requerir la concurrencia de "k" para la activación y uso del módulo que contiene dichas claves. Un control similar se realiza dentro de Autoridad de Certificación Raíz de El Salvador.

6.2.3. Controles sobre la clave privada de la AC

6.2.3.1. Copia de seguridad de la clave privada

Las copias de respaldo de las claves privadas se almacenan cifradas en el sitio alterno al centro de datos de San Salvador.

Existe por lo menos una copia de respaldo de las claves privadas de la AC que permite su recuperación en caso de desastre, la misma que es almacenada y recuperada por el personal autorizado según los roles de confianza, y con la presencia de una custodia de claves.

6.2.3.2. Archivo de la clave privada

Las claves privadas de las Autoridad de Certificación se guardan en dispositivos de hardware criptográfico con certificación que aseguren los niveles de seguridad e integridad reflejados en esta DPC.

6.2.3.3. Introducción de la clave privada al módulo criptográfico

La clave privada se crea dentro del módulo criptográfico en el momento de la creación de cada una de las Autoridades de Certificación que hace uso de dichos módulos.

6.2.3.4. Activación de la clave privada

Los métodos de activación deben contar con mecanismos de autenticación de al menos dos factores de seguridad. Los datos de activación deben estar distribuidos en roles de confianza que ejecutan diversas personas.

6.2.3.5. Desactivación de la clave privada

En el caso de las claves privadas de PSC o TSA que se encuentren on-line, la desactivación debe ocurrir al momento del apagado del módulo criptográfico que las contiene, lo cual deberá estar reflejado en el respectivo procedimiento.

6.2.3.6. Destrucción de clave privada

En caso se requiera la destrucción de una clave privada por parte de un PSC o TSA, primero deberá realizarse el procedimiento de revocación del certificado digital y luego se debe eliminar su clave privada del módulo criptográfico correspondiente, para lo cual debe tener un procedimiento aprobado. El procedimiento debe asegurar que copias recuperables no se mantengan en el dispositivo criptográfico o en zonas de memoria o de disco, incluyendo cualquier copia de seguridad. Además, se debe custodiar los registros de la destrucción de la clave privada.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

Las claves públicas o los certificados que las contengan, deben ser archivadas.

6.3.2. Periodos operacionales del certificado y periodos de uso del par de claves

El periodo operacional y de uso del par de claves se determina de acuerdo al en el periodo de validez del certificado digital de PSC o TSA. Dicho periodo se encuentra comprendido en el intervalo entre los campos *NotBefore* (inicio de la validez) y *NotAfter* (fin de la validez), siempre y cuando el PSC o TSA se encuentre habilitado para poder operar.

6.4. Datos de activación

Los proveedores de servicios de certificación deben mantener sus datos de activación bajo controles estrictos, siendo de acceso solamente a los roles de confianza definidos.

6.5. Controles de seguridad informática

Los controles de seguridad informática establecidos en la Unidad de Firma Electrónica se consideran información sensible y confidencial. No obstante, se señalan los siguientes aspectos:

- Control de acceso a los servicios de la AC.
- Identificación y autenticación de usuarios para las aplicaciones de la AC a partir de certificados digitales.
- Auditoría de eventos relativos a la seguridad.
- Mecanismos de recuperación de claves y del sistema de la AC.
- Configuración de seguridad de las aplicaciones.
- Configuración de usuarios y privilegios.
- Gestión de privilegios para asignar las tareas según el rol.
- Plan de administración y mantenimiento del sistema de alta disponibilidad.
- Plan de contingencia y recuperación de desastres.

6.6. Controles técnicos de seguridad del ciclo de vida

Los controles de desarrollo del sistema incluyen la seguridad de la gestión de configuración, las prácticas de ingeniería de software en los entornos de test y contingencia.

6.7. Controles de seguridad de la red

Los módulos criptográficos de la Autoridad de Certificación Raíz se encuentran sin energía y, fuera de la red y en modo *offline*. Asimismo, los equipos donde se despliegan los repositorios de la Unidad de Firma Electrónica se encuentran protegidos contra ataques, accesos no autorizados o alteración de datos.

7 Perfiles de Certificados y Listas de Revocación

7.1. Perfiles de certificado

El contenido del certificado raíz del Ministerio de Economía es el siguiente:

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Identifier	1.2.840.113549.1.1.13		
1.3.2. Algorithm	Sha512WithRSAEncryption	Sí	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"SV"	Sí	
1.4.2. Locality Name (L)	"SAN SALVADOR"	Sí	
1.4.3. Organizational Unit (OU)	"UNIDAD DE FIRMA ELECTRONICA"	Sí	
1.4.4. Organization Name (O)	"MINISTERIO DE ECONOMIA"	Sí	
1.4.5. Common Name (CN)	"AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR"	Sí	
1.4.6. Organization Identifier (other name)	"VATSV-06140101140073"	Sí	
1.5. Validity	**(25 años)**	Sí	
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado (codificado en UTCTime)	Sí	

Campo	Contenido	Obligatorio	Crítico
1.5.2. Not After	Fecha y hora de expiración del certificado (codificado en UTCTime) notBefore + 25 años	Sí	
1.6. Subject		Sí	
1.6.1. Country Name	"SV"	Sí	
1.6.2. Locality Name (L)	"SAN SALVADOR"	Sí	
1.6.3. Organizational Unit (OU)	"UNIDAD DE FIRMA ELECTRONICA"	Sí	
1.6.4. Organization Name (O)	"MINISTERIO DE ECONOMIA"	Sí	
1.6.5. Common Name (CN)	"AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR"	Sí	
1.6.6. Organization Identifier (OID 2.5.4.97)	"VATSV-06140101140073"	Sí	
1.7. Subject Public Key Info		Sí	
1.7.1. AlgorithmIdentifier	1.2.840.113549.1.1.1		
1.7.1.1. Algorithm	RSA encryption	Sí	
1.7.1.2. Parameters	No aplicable	No	
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 4096 bits	Sí	
2. Extensions			
2.1. Authority Key Identifier		Sí	No
2.1.1. KeyIdentifier	Identificador de la clave del emisor	Sí	

Campo	Contenido	Obligatorio	Crítico
2.2. Subject Key Identifier		Sí	No
2.2.1. KeyIdentifier	Identificador de la clave del subject	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado "0"		
2.3.2. Content commintment	No seleccionado "0"		
2.3.3. Key Encipherment	No seleccionado "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	Seleccionado "1"	Sí	
2.3.7. CRL Signature	Seleccionado "1"	Sí	
2.3.8. Encipher Only	No seleccionado. "0"		
2.3.9. Decipher Only	No seleccionado. "0"		
2.4. Certificate Policies		Si	No
2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	2.5.29.32.0	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.2. 1 CPS URI	URL del directorio donde se encuentra la DPC.	Sí	

Campo	Contenido	Obligatorio	Crítico
	(https://normativa.firmaelectronica.economia.gob.sv/dpc/)		
2.4.1.1. 2. User Notice/Explicit text	AUTORIDAD REGISTRADORA Y ACREDITADORA RAIZ EL SALVADOR	Sí	
2.4.2. Policy Information		No	
2.4.2.1. Policy Identifier		No	
2.5. Subject Alternative Names		Sí	No
2.5.1. rfc822Name	Email de la CA (firma.electronica@economia.gob.sv)	Sí	
2.6 Issuer Alternative Name			
2.6.1 rfc822Name	Email de la CA (firma.electronica@economia.gob.sv)	No	
2.7 Basic Constraints		Sí	
2.7.1 Subject type	CA (VERDADERO)	Sí	
2.7.2 Path Length Constraints	Ninguno	Sí	

El contenido de los certificados de un PSC o TSA es el siguiente:

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí	
1.3. Signature Algorithm		Sí	

Campo	Contenido	Obligatorio	Crítico
1.3.1 Identifier	1.2.840.113549.1.1.13		
1.3.2. Algorithm	Sha512WithRSAEncryption	Sí	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"SV"	Sí	
1.4.2. Locality Name (L)	"SAN SALVADOR"	Sí	
1.4.3. Organizational Unit (OU)	"UNIDAD DE FIRMA ELECTRONICA"	Sí	
1.4.4. Organization Name (O)	"MINISTERIO DE ECONOMIA"	Sí	
1.4.5. Common Name (CN)	"AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR"	Sí	
1.4.6. Organization Identifier (other name)	"VATSV-06140101140073"	Sí	
1.5. Validity	**(15 años)**	Sí	
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado (codificado en UTCTime)	Sí	
1.5.2. Not After	Fecha y hora de expiración del certificado (codificado en UTCTime) NotBefore + 15 años	Sí	
1.6. Subject		Sí	
1.6.1. Country Name	"SV"	Sí	
1.6.2. Locality Name (L)	Nombre de la LOCALIDAD del domicilio del PSC o TSA (No incluir información adicional al nombre de la localidad)	Sí	
1.6.3. Organizational Unit (OU)	UNIDAD ORGANIZATIVA CA SUBORDINADA	Sí	
1.6.4. Organization Name (O)	ORGANIZACIÓN CA SUBORDINADA	Sí	
1.6.5. Common Name (CN)	NOMBRE DE LA CA SUBORDINADA	Sí	

Campo	Contenido	Obligatorio	Crítico
1.6.6. Organization Identifier (other name)	"VATSV-[NIT CA SUBORDINADA]"	Sí	
1.7. Subject Public Key Info		Sí	
1.7.1. AlgorithmIdentifier	1.2.840.113549.1.1.1		
1.7.1.1. Alg orithm	RSA encryption	Sí	
1.7.1.2. Par ameters	No aplicable	No	
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 4096 bits	Sí	
2. Extensions			
2.1. Authority Key Identifier		Sí	No
2.1.1. KeyIdentifier	Identificador de la clave del emisor	Sí	
2.2. Subject Key Identifier		Sí	No
2.2.1. KeyIdentifier	Identificador de la clave del subject	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado "0"		
2.3.2. Content commintment	No seleccionado "0"		
2.3.3. Key Encipherment	No seleccionado "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		

Campo	Contenido	Obligatorio	Crítico
2.3.6. Key Certificate Signature	Seleccionado "1"	Sí	
2.3.7. CRL Signature	Seleccionado "1"	Sí	
2.3.8. Encipher Only	No seleccionado. "0"		
2.3.9. Decipher Only	No seleccionado. "0"		
2.4. Certificate Policies		Si	No
2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	1.3.6.1.4.1.50377.1.1.1	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1 .1. CPS URI	URL donde se encuentra la DPC. (http://normativa.firmaelectronica.economia.gob.sv/dpc/)	Sí	
2.4.1.1 .2. User Notice/Explicit text	Certificado de la autoridad subordinada proveedor de servicios de certificación	Sí	
2.4.2. Policy Information		No	
2.4.2.1. Policy Identifier		No	
2.5. Subject Alternative Names		No	No
2.5.1. rfc822Name	Email de la CA Subordinada (Ej. info@ca-subordinada.sv)	No	
2.6. cRLDistributionPoint		Sí	Sí

Campo	Contenido	Obligatorio	Crítico
2.6.1. distributionPoint	URL donde se encuentra la ARL (CRL de la CA Raíz) Ej. http://crl1.firmaelectronica.minec.gob.sv/crl/arl_minec.crl	Sí	
2.6.2. distributionPoint	URL alterna donde se encuentra la ARL (CRL de la CA Raíz) Ej. http://crl2.firmaelectronica.minec.gob.sv/crl/arl_minec.crl	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. Subject type	CA (VERDADERO)	Sí	
2.7.2 Path Length Constraints	Ninguno	Sí	

7.1.1. Número de versión

El formato de los distintos tipos de certificados emitidos por la CA Raíz y la CA Subordinada de la jerarquía raíz de El Salvador, incluyendo los certificados autofirmados de la CA Raíz, será X.509 v3, conforme al estándar RFC 5280.

7.1.2. Extensiones del certificado

Podrán incluir únicamente las extensiones de certificado definidas en [RFC5280] que están indicadas en los perfiles de certificado especificados en Perfiles de Certificados definidos por la Unidad de Firma Electrónica como pueden ser:

- authorityKeyIdentifier
- subjectKeyIdentifier
- keyUsage
- certificatePolicies
- subjectAltName
- basicConstraints
- extKeyUsage
- cRLDistributionPoints

- authorityInformationAccess

7.1.3. Identificadores de objeto del algoritmo

Los PSC o TSA utilizarán la estructura de OID definida por la Unidad de Firma electrónica, podrán también declarar, de forma adicional, los OID de aquellas políticas de línea base a las que se adhieran a efectos de interoperabilidad, como ETSI EN 319 411-1.

7.1.4. Formatos de nombres

Se debe respetar la forma de nombres de acuerdo a la familia de estándares ISO/IEC 9594 (recomendación X.500) para *DistinguishedName* como se especifica en el numeral **3.1.1 Tipos de Nombres.**

7.1.5. Restricciones de nombre

De acuerdo a la recomendación X.500 para nombres en certificados digitales estos deben ser únicos y no ambiguos.

7.1.6. Objeto identificador de la Política de Certificados

Los PSC o TSA utilizarán la estructura de OID definida por la Unidad de Firma electrónica, podrán también declarar, de forma adicional, los OID de aquellas políticas de línea base a las que se adhieran a efectos de interoperabilidad, como ETSI EN 319 411-1.

7.1.7. Sintaxis y semántica de los calificadores de la política

La extensión de los certificados referente a los calificadores de la Política de Certificados contiene la siguiente información:

- *CertificatePolicy*: Contiene la Política de Certificados de proveedores de servicios de certificación.

7.2. Perfil de las Listas de Certificados Revocados CRL

El formato de las CRL emitidas por la CA Raíz (ARL) y la CA Subordinada será X.509 v2, conforme al estándar [RFC5280], con las siguientes restricciones en sus componentes:

ARL de Autoridad de Certificación raíz:

ARL MINEC	
Componente	**Valor**
Campos de CRL X.509 v2 (tbsCertList)	
version	"1"
signature	
algorithm	sha256withRSAEncryption
issuer	
countryName (C)	"SV"
localityName (L)	"SAN SALVADOR"
organizationalUnitName (OU)	"UNIDAD DE FIRMA ELECTRONICA"
organizationName (O)	"MINISTERIO DE ECONOMIA"
commonName (CN)	"AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR"
otherName	"VATSV-06140101140073"
thisUpdate	Fecha y hora de emisión de la CRL, codificado en UTCTime
nextUpdate	thisUpdate + 6 meses, codificado en UTCTime
Certificados revocados en CRL X.509 v2 (revokedCertificates)[4]	
userCertificate	Valor del campo serialNumber del certificado revocado
revocationDate	Fecha y hora de revocación del certificado, codificado en UTCTime
crlEntryExtensions	
reasonCode	Motivo de revocación del certificado (uno de los valores): unspecified; keyCompromise; keyCompromise; affiliationChanged; superseded; cessationOfOperation; certificateHold; privilegeWithdrawn; aACompromise
Extensiones de CRL X.509 v2 (crlExtensions)	
authorityKeyIdentifier	
keyIdentifier	Valor en extensión subjectKeyIdentifier del certificado de CA Raíz MINEC
cRLNumber	Número entero secuencial (valor inicial: 00)

[4] Lista de entradas, una por cada certificado revocado, cada una de ellas con los 3 componentes indicados.

CRL de PSC o TSA:

CRL (CA SUBORDINADAS)	
Componente	**Valor**
Campos de CRL X.509 v2 (tbsCertList)	
version	"1"
signature	
algorithm	sha256withRSAEncryption
issuer	
countryName (C)	"SV"
localityName (L)	Nombre de la LOCALIDAD/(DEPARTAMENTO) donde resida el proveedor del servicio de certificación. (No incluir información adicional al nombre de la localidad)
organizationalUnitName (OU)	UNIDAD ORGANIZATIVA CA SUBORDINADA
organizationName (O)	ORGANIZACIÓN CA SUBORDINADA
commonName (CN)	NOMBRE DE LA CA SUBORDINADA
otherName	"VATSV-[NIT _PROVEEDOR]"
thisUpdate	Fecha y hora de emisión de la CRL, codificado en UTCTime
nextUpdate	thisUpdate + 1 día, codificado en UTCTime
Certificados revocados en CRL X.509 v2 (revokedCertificates)[5]	
userCertificate	Valor del campo serialNumber del certificado revocado
revocationDate	Fecha y hora de revocación del certificado, codificado en UTCTime
crlEntryExtensions	
reasonCode	Motivo de revocación del certificado (uno de los valores): unspecified; keyCompromise; keyCompromise; affiliationChanged; superseded; cessationOfOperation; certificateHold; privilegeWithdrawn; aACompromise
Extensiones de CRL X.509 v2 (crlExtensions)	
authorityKeyIdentifier	
keyIdentifier	Valor en extensión subjectKeyIdentifier del certificado de CA Subordinada
cRLNumber	Número entero secuencial (valor inicial: 00)

[5] Lista de entradas, una por cada certificado revocado, cada una de ellas con los 3 componentes indicados.

7.2.1. Número de versión

Se debe implementar al menos el perfil de CRL en su versión 2 (X.509 v2) en conformidad con lo especificado en la RFC 5280 "PKIX Certificate and CRL Profile".

7.2.2. Extensiones de las CRL

authorityKeyIdentifier
keyIdentifier
cRLNumber

Extensiones de CRL (componentes del elemento crlExtensions, en el componente tbsCertList de las CRL), de acuerdo al numeral **7.2 Perfil de Listas de Certificados Revocados.**

8 Auditorías de Conformidad y otras Valoraciones

8.1. Frecuencia y circunstancias de las auditorías

Los PSC o TSA se deben someter a una auditoría anual, de conformidad con los lineamientos dictados por la Unidad de Firma Electrónica.

8.2. Identidad y calificaciones de los auditores

Los auditores serán designados por la Unidad de Firma Electrónica, de acuerdo a los procedimientos que esta establezca. Adicionalmente, la Unidad de Firma Electrónica está en la potestad de realizar visitas no programadas de inspección a cualquiera de los Proveedores de Servicios de Certificación acreditados en El Salvador.

8.3. Relación entre el auditor y la entidad evaluada

No deberá existir relación de ningún tipo entre el PSC o TSA auditado y el auditor, ni ninguna otra circunstancia que pudiese derivar en conflicto de intereses que comprometiese la imparcialidad de la auditoría.

8.4. Temas cubiertos en la valoración

Se procederá a auditar, como mínimo, los siguientes aspectos considerados como críticos:

- Alineación de procedimientos con la de la Declaraciones de Prácticas y las Políticas de Certificación
- Evaluación y cumplimiento de los niveles de seguridad
- Revisión de los procedimientos de contingencia
- Revisión del Plan de Contingencias
- Revisión de los controles de seguridad de la información

8.5. No conformidades

Al detectarse una irregularidad (no conformidad), podrán tomarse entre otras las siguientes acciones:

- Indicar las no conformidades detectadas, requiriendo un plan de medidas preventivas por partes del PSC o TSA.
- Suspensión de la operación del PSC o TSA y la consiguiente revocación del certificado digital.

El auditor entregará al PSC o TSA un dictamen de auditoría sustentando las no conformidades detectadas, basando la severidad de las mismas a los riesgos e impacto sobre la seguridad y confianza de los suscriptores y titulares, en base al cual el PSC o TSA deberá tomar las medidas correspondientes a la severidad de las no conformidades, si las hubiese.

Una vez subsanadas las no conformidades, o presentado el plan de medidas preventivas o correctivas sobre las no conformidades, el auditor procederá a emitir el dictamen correspondiente.

8.6. Comunicación de resultados

La comunicación de los resultados de la auditoría será responsabilidad de la Unidad de Firma Electrónica, debiendo realizarla dentro de plazos establecidos en los procedimientos que esta estalezca.

9 Otros Asuntos Comerciales y Legales

9.1. Responsabilidad financiera

Los proveedores de servicios de certificación deberán mantener una póliza de responsabilidad civil para responder ante cualquier eventualidad que signifique un perjuicio para los suscriptores, siempre y cuando los daños y perjuicios se deriven de errores, omisiones o actos negligentes por parte de los proveedores.

Se aclara que la Unidad de Firma Electrónica no se responsabiliza por actos relacionados con el incumplimiento o ejecución incorrecta de las obligaciones contraídas por el suscriptor y/o usuario de un certificado de firma, y por la incorrecta utilización de los certificados digitales y claves privadas.

9.2. Información confidencial de los negocios

La Unidad de Firma Electrónica garantiza que la información entre los usuarios de los certificados de firma y terceros que confían, tales como planes de negocios, información de ventas, secretos comerciales y otros, es confidencial y de uso exclusivo por parte de los interesados.

9.3. Alcance de la información confidencial

La Unidad de Firma Electrónica considera como información confidencial que no podrá ser divulgada a terceros a:

- Las claves privadas de los PSC o TSA, mismas que están en control del PSC o TSA.
- La información de suscriptores que no está contenida en el certificado digital.
- La información relativa a las operaciones que lleva a cabo la Unidad de Firma Electrónica.
- La información acerca de los parámetros de seguridad, controles y procedimientos de auditoría. Manual de seguridad y procedimientos internos de la Unidad de Firma Electrónica o cualquier otro que entregarán los proveedores de servicios de certificación durante el proceso de acreditación, exceptuando aquella información o documentación pública que se incorpore al expediente administrativo.

9.4. Información no confidencial

La información que no se considera confidencial hace referencia a:

- La incluida en la Declaración de Prácticas de Certificación de la jerarquía raíz y de los proveedores de servicios de certificación.

- La incluida en las Políticas de Certificación de los diferentes tipos de certificados emitidos en El Salvador.
- Las listas de certificados revocados (CRL).
- Cualquier otra información pública.

9.5. Responsabilidad para proteger la información confidencial

El personal de la Unidad de Firma Electrónica que participa en las actividades relativas al funcionamiento de la infraestructura para la emisión de certificados está sujeto al deber de secreto de acuerdo a las políticas de la Unidad de Firma Electrónica para su contratación y desempeño.

9.6. Plan de privacidad

El plan de privacidad desarrollado para proteger la información considerada confidencial incluye controles para proteger y precautelar su integridad, así también, para asignarle el nivel de criticidad correspondiente.

9.7. Notificación y consentimiento para el uso de información privada

Se requiere del consentimiento expreso del dueño de la información para el uso de la información privada o confidencial.

9.8. Divulgación de información dentro de un proceso judicial o administrativo

Únicamente por requerimiento de las autoridades dentro de un proceso judicial o administrativo la Unidad de Firma Electrónica hará entrega a terceros de la información catalogada como confidencial por parte de los suscriptores.

9.9. Derechos de propiedad intelectual

Los derechos de propiedad intelectual, tales como derechos de autor, patentes, marcas registradas o secretos comerciales que los suscriptores declaran como tales o que están incluidos en los certificados, nombres, claves, DPC o PC, son protegidos por la Unidad de Firma Electrónica.

El suscriptor conserva la propiedad intelectual sobre las claves privadas y públicas relativas a su certificado.

9.10. Plazo y terminación

La Declaración de Prácticas de Certificación y cada una de las Políticas de Certificado entran en vigor desde el momento en que se publican en la página web de cada PSC y TSA o de la misma Unidad de Firma Electrónica, a partir de ese momento la versión anterior del documento queda derogada y la nueva versión reemplaza íntegramente la versión anterior. Se conserva en el repositorio las anteriores versiones de la DPC y de cada PC.

9.11. Notificación individual e información a los participantes

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta DPC se realizará mediante correos electrónicos, a través de la página web de la Unidad de Firma Electrónica, notas de prensa o cualquier otro mecanismo.

9.12. Modificaciones en las DPC y PC

Se establece un control de modificaciones, basado en la Política de Gestión de Cambios de la Unidad de Firma Electrónica.

9.13. Prevención y resolución de controversias

Si una controversia entre las partes surge o se relaciona con la presente Declaración de Prácticas de Certificación, el incumplimiento de las estipulaciones en ella contenidas, o cualquier actuación u obligación debida por la presente, y si la controversia no puede ser resuelta a través de arreglo directo, agotada esta vía si la controversia persistiere las partes recurrirán al arbitraje de conformidad con las normas y leyes salvadoreñas.