POLÍTICA DE CERTIFICADOS PARA LA JERARQUÍA NACIONAL DE CERTIFICADORES REGISTRADOS

Dirección de Gobernanza Digital
Certificadores de Firma Digital
Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones

OID: 2.16.188.1.1.1.1
Versión: 2.0
04 de abril, 2022


micitt
MINISTERIO DE CIENCIA,
INNOVACIÓN, TECNOLOGÍA
Y TELECOMUNICACIONES

Control de versiones

Fecha	Versión	Autor(es)	Aprobado	Descripción
26-10-07	Consulta pública	Comité de Políticas Comité Técnico	Lic. Oscar Solís Director DCFD	Se presenta la versión para discusión final del comité de políticas y aprobación del Director de la DCFD.
03-12-07	Borrador	Comité de Políticas	Lic. Oscar Solís Director DCFD	Se incorporan las observaciones de la consulta pública, de acuerdo al edicto publicado el día lunes 19 de noviembre del 2007 en el diario oficial La Gaceta Nº 222.
04-09-08	1.0	Comité de Políticas	Lic. Oscar Solís Director DCFD	Oficialización y entrada en vigencia de la política.
03-04-13	Consulta pública (1.1)	Comité de Políticas Dirección de Certificadores de Firma Digital	Alexander Barquero Director DCFD	Actualizaciones para certificados digitales de persona jurídica, vigencia y unicidad de los certificados.
10-05-13	Borrador (1.1)	Dirección de Certificadores de Firma Digital	Alexander Barquero Director DCFD	Se incorporan las observaciones de la consulta pública, de acuerdo al aviso del martes 16 de abril del 2013 en el Alcance Digital Nº 68 del diario oficial La Gaceta Nº 72.
20-05-13	1.1	Dirección de Certificadores de Firma Digital	Alexander Barquero Director DCFD	Oficialización y entrada en vigencia de la versión 1.1 de la política.
23-08-17	Consulta pública (1.2)	Dirección de Certificadores de Firma Digital	Alexander Barquero Director DCFD	Actualizaciones para gestión de llaves privadas de los certificados digitales de persona jurídica.
08-09-17	Borrador	Dirección de Certificadores de Firma Digital	Alexander Barquero Director DCFD	Se incorporan las observaciones de la consulta pública.
21-02-18	1.2	Dirección de Gobernanza Digital (Departamento de Certificadores de Firma Digital)	Alexander Barquero Director DGD	Oficialización y entrada en vigencia de la versión 1.2 de la política.
04-04-2022	2.0	Dirección de Gobernanza Digital, Certificadores de Firma Digital	Jorge Mora Flores Director DGD	Se realizan modificaciones en las siguientes secciones: 1.Introducción 1.4.2 Usos prohibidos del certificado 2.2 Publicación de información de certificación 3.1.1 Tipos de nombres, en la sección de persona jurídica 3.2.1 Método para probar posesión de la llave privada 3.2.3 Autenticación de identidad de persona física 3.2.6 Criterios para interoperabilidad 3.4 Identificación y autenticación para solicitudes de Revocación 4.1 Solicitud de certificado 4.1.2 Proceso de inscripción y responsabilidades 4.3.2 Notificación al suscriptor por parte de la CA sobre la emisión del certificado 4.9 Revocación y suspensión de certificado 4.9.7 Frecuencia de emisión de CRL 4.9.14 Quién puede solicitar la suspensión 4.9.15 Procedimiento para la solicitud de suspensión 4.12 Custodia y recuperación de llave 5.3.2 Procedimientos de verificación de antecedentes 5.3.5 Frecuencia y secuencia en la rotación de las funciones 5.6 Cambio de llave 6.1.1 Generación del par de llaves 6.1.5 Tamaños de llave

				6.2.1 Estándares y controles del módulo criptográfico 6.2.3 Custodia de llave privada 6.2.4 Respaldo de llave privada 6.2.8 Método de activación de llave privada 6.2.10 Método de destrucción de llave privada 6.2.11 Clasificación del módulo criptográfico 6.3.2 Periodo operacional del certificado y periodo de uso del par de llaves 7.1 Perfil del Certificado 7.1.2.5 Uso extendido de la llave 7.1.3 Identificadores de objeto de algoritmos 7.2 Perfil de la CRL 8.4 Aspectos cubiertos por la Evaluación 9.5 Derechos de propiedad intelectual Se ajusta la forma para la sección de Definiciones y acrónimos, eliminándola de Anexos. Se actualiza el nombre del Ministerio y sus logos.

JORGE EMILIO MORA FLORES (FIRMA)

Firmado digitalmente por JORGE EMILIO MORA FLORES (FIRMA)
Fecha: 2022.05.07 21:38:17 -06'00'

Director de Gobernanza Digital
Ministerio de Ciencia, Innovación, Tecnología Telecomunicaciones

Índice

1. Introducción

Este documento define las Políticas de Certificado (en adelante CP) dictadas por la Dirección de Gobernanza Digital (en adelante DGD) para el Sistema Nacional de Certificación Digital.
La autoridad certificadora registrada debe implementar las políticas en los servicios de certificación que incluyen: la emisión, gestión, suspensión y revocación de los certificados.
Las siguientes secciones describen las políticas de acatamiento obligatorio que deben ser implementadas por la Autoridad Certificadora Raíz (en adelante CA Raíz) y por cualquier otra Autoridad Certificadora Registrada (en adelante CA) en los niveles inferiores de la jerarquía nacional de certificadores registrados. Sin embargo, este documento no pretende ser una guía exhaustiva para la evaluación del cumplimiento de los requisitos necesarios para un proceso de acreditación. La guía detallada para la evaluación de una autoridad certificadora que desea incorporarse al Sistema de Certificación Nacional debe solicitarse a la DGD, y la misma se adhiere a los lineamientos establecidos en: la norma INTE-ISO-21188 "Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas" versión vigente o el estándar Trust Service Principles and Criteria for Certification Authorities Version vigente – Webtrust.

Esta CP se ha desarrollado conforme a lo estipulado en el RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".

1.1 Resumen

Estas Políticas de Certificado (CP) son específicamente aplicables a:

- Autoridad Certificadora Raíz (CA Raíz).
- Autoridades Certificadoras de Políticas (CA de Políticas) dentro de la jerarquía nacional de certificadores registrados.
- Autoridades Certificadoras emisoras (CA emisoras) que se registren ante la DGD, y que emitan los certificados a las entidades finales.
- Suscriptores y partes que confían.

Las políticas nacionales contemplan los siguientes tipos de certificados, definidos en este documento como:

- Certificados para CA emisoras.
- Certificados de autenticación de persona física.
- Certificados de firma digital de persona física.
- Certificados de agente electrónico (autenticación) de persona jurídica.
- Certificados de sello electrónico (firma digital) de persona jurídica.
- Certificados de autoridades de estampado de tiempo (TSA).

Los diferentes tipos de certificados están definidos en la política y se implementan a través de una jerarquía de tres niveles: el primero corresponde a la raíz nacional, el segundo nivel corresponde a las autoridades certificadoras de políticas y el tercer nivel a las CA emisoras de certificados.
El siguiente diagrama detalla la estructura de la jerarquía nacional de certificadores registrados:

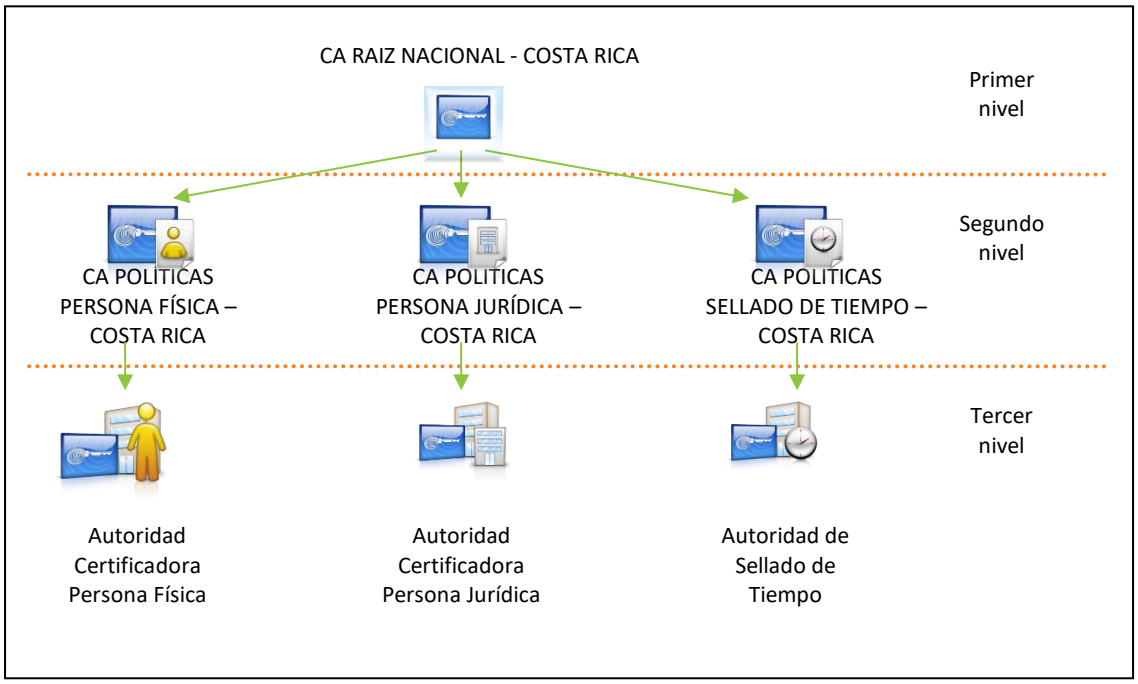

Diagrama de la jerarquía nacional de certificadores registrados

1.2 Nombre e identificación del documento

Este documento es la "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados" y se referencia mediante el identificador de objeto (OID): 2.16.188.1.1.1.1

Sección	Descripción
2	joint-iso-itu-t
16	Country
188	Costa Rica
1	Organización
1	Dirección de Certificadores de Firma Digital
1	Políticas
1	Política de Certificados para la jerarquía nacional de certificadores registrados

Las políticas derivadas para la jerarquía nacional de certificadores registrados son:

Política para certificados generados por la jerarquía nacional de certificadores registrados	OID
Política de certificados de CA emisora del Sistema Nacional de Certificación Digital	2.16.188.1.1.1.1.1
Política de certificados de persona física del Sistema Nacional de Certificación Digital • Firma digital • Autenticación	 2.16.188.1.1.1.1.2 2.16.188.1.1.1.1.3
Política de sellado de tiempo del Sistema Nacional de Certificación Digital	2.16.188.1.1.1.1.5
Política de certificados de persona jurídica del Sistema Nacional de Certificación Digital • Sello electrónico • Agente electrónico	 2.16.188.1.1.1.1.6 2.16.188.1.1.1.1.7

1.3 Participantes en la PKI

1.3.1 Autoridades certificadoras

Las autoridades certificadoras (CA) son todas las entidades autorizadas a emitir certificados de llave pública dentro de la jerarquía nacional de certificadores registrados. Esto incluye:

- CA Raíz.
- CA de Políticas.
- CA emisoras.

La CA Raíz y las CAs de Políticas son parte de la jerarquía nacional administrada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). Ambas se regulan a través de la Dirección de Gobernanza Digital (DGD). Las CAs emisoras deben implementar esta política, para formar parte de la jerarquía nacional de certificadores registrados.

1.3.2 Autoridades de Registro

Una Autoridad de Registro (RA) es una entidad que verifica la identidad de los solicitantes que aplican por un certificado. La RA debe validar los requisitos de identificación del solicitante, dependiendo del tipo de certificado y de la especificación de la política pertinente. Además, tramita las solicitudes de revocación para los certificados y valida la información contenida en las solicitudes de certificados. Las Autoridades de Registro se regulan en el documento de "Directrices para las Autoridades de Registro. Características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica" emitido por la DGD para este propósito.

1.3.3 Suscriptores

Se define como suscriptor a todos los usuarios finales a quienes se les ha emitido un certificado por una CA, dentro de la jerarquía nacional de certificadores registrados. El suscriptor puede ser una persona física o una persona jurídica.

1.3.4 Partes que confían

Una parte que confía es una persona física o jurídica que actúa confiando en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos bajo la jerarquía nacional de certificadores registrados. Una parte que confía puede o no ser también un suscriptor.

1.3.5 Otros participantes

Sin estipulaciones.

1.4 Uso del certificado

1.4.1 Usos apropiados del certificado

Tipo	Descripción de uso apropiado
Certificados de CA emisora	• Operar la infraestructura PKI y emitir certificados a suscriptores dentro de la cadena de confianza. ○ Digital Signature. ○ Certificate Signing. ○ Off-line CRL Signing. ○ CRL Signing.
Certificados de firma digital de persona física	• Firma digital ○ Digital Signature.

	○ Non-Repudiation.
Certificados de autenticación de persona física	• Autenticación ○ Digital Signature. ○ Key Encipherment.
Certificados de sello electrónico de persona jurídica	• Sello electrónico ○ Digital Signature. ○ Non-Repudiation.
Certificados de agente electrónico de persona jurídica	• Agente electrónico ○ Digital Signature. ○ Key Encipherment. ○ Data Encipherment.
Certificados de Autoridad de Sellado de Tiempo (TSA)	• Sellado de tiempo ○ Digital Signature. ○ Non-Repudiation.

1.4.2 Usos prohibidos del certificado

Los certificados emitidos deben ser utilizados dentro del marco de la Ley N°8454 "Ley de certificados, firmas digitales y documentos electrónicos" y su reglamento. Cualquier otro uso del certificado no especificado en la Ley N°8454, su reglamento y en esta CP (y sus políticas asociadas) está fuera del alcance y responsabilidad de estas políticas.

El certificado de autenticación del suscriptor no debe ser usado para la creación de firmas digitales certificadas, a excepción de su uso en el proceso de autorización para activar el uso de llaves en la firma digital remota de documentos.

1.5 Administración de la Política

1.5.1 Organización que administra el documento

Dirección de Gobernanza Digital, Certificadores de Firma Digital

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, dirección: San José, San José, Zapote, 400 metros oeste de Casa Presidencial Edificio Mira, primer piso. Apartado Postal: 5589-1000 San José, Costa Rica.

1.5.2 Persona de contacto

Director de Gobernanza Digital, Certificadores de Firma Digital. Correo Electrónico: firmadigital@micitt.go.cr. Tel. (506)2539-2201, ext. 2243 o 2261.

1.5.3 Persona que determina la adecuación de la CPS a la Política

El Director de la Dirección de Gobernanza Digital será el encargado de determinar la adecuación de la declaración de prácticas de certificación (CPS) de todas las autoridades certificadoras que desean pertenecer a la jerarquía nacional de certificadores registrados.

1.5.4 Procedimientos de aprobación de la CP

La política y las subsecuentes enmiendas o modificaciones deben ser propuestas por la DGD o por el Comité Asesor de Políticas, y presentadas al Director de la DGD, quien posterior a su análisis y correcciones, las somete a consulta pública (salvo casos de urgencia) en la que se invitará a las entidades públicas y privadas, organizaciones representativas y público en general a

ofrecer comentarios y sugerencias pertinentes; todo conforme a los artículo 361[1] y 362[2] de la Ley General de Administración Pública (LGAP). La encargada de la aprobación final de la CP es la DGD.

1.6 Definiciones y abreviaturas

Definiciones

Términos	Definición
Acuerdo de parte que confía, RPA (por sus siglas en inglés Relying party agreement)	Es un acuerdo entre la autoridad certificadora y las partes que confían que típicamente establece los derechos y responsabilidades entre estas partes con respecto a la verificación de las firmas digitales y otros usos del certificado. Este acuerdo no requiere la aceptación explícita de la parte que confía.
Acuerdo de suscriptor	Es un acuerdo entre la CA raíz y la CA emisora, y entre la CA emisora y el suscriptor, que establece los derechos y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Este acuerdo sí requiere la aceptación explícita tanto de la CA emisora como del suscriptor, respectivamente.
Agente electrónico	Certificado de autenticación de persona jurídica; se suelen utilizar como parte de un proceso automático de autenticación (prueba de identidad) entre sistemas automatizados, en donde el dispositivo criptográfico que contiene las llaves asociadas al certificado está activo para que pueda trabajar en forma desatendida y de esta manera no requiera de intervención humana cada vez que se requiere de su uso.
Apoderado	Persona que tiene la capacidad jurídica para actuar en nombre de una empresa o institución y que tiene la potestad legal para cumplir con las responsabilidades asignadas en este CP.
Autenticación	Verificación de la identidad afirmada por el individuo: a) en el momento de registro, el acto de evaluar las credenciales de las entidades finales (esto es, suscriptores) como evidencia de la identidad afirmada; b) durante su uso, el acto de comparar electrónicamente la identidad y las credenciales presentadas contra los valores almacenados, para probar identidad.
Autoridad Certificadora CA (por sus siglas en inglés)	Entidad en la cual una o más entidades confían para crear, asignar, revocar o suspender certificados de llave pública.
Autoridad Certificadora Registrada	El certificador inscrito y autorizado por la Dirección de Gobernanza Digital.

1 Artículo 361.-

1. Se concederá audiencia a las entidades descentralizadas sobre los proyectos de disposiciones generales que puedan afectarlas.
2. Se concederá a las entidades representativas de intereses de carácter general o corporativo afectados por la disposición la oportunidad de exponer su parecer, dentro del plazo de diez días, salvo cuando se opongan a ello razones de interés público o de urgencia debidamente consignadas en el anteproyecto.
3. Cuando, a juicio del Poder Ejecutivo o del Ministerio, la naturaleza de la disposición lo aconseje, el anteproyecto será sometido a la información pública, durante el plazo que en cada caso se señale.

2 Artículo 362.- En la disposición general se han de consignar expresamente las anteriores que quedan total o parcialmente reformadas o derogadas.

Términos	Definición
Autoridad de políticas PA (por sus siglas en inglés)	Parte o cuerpo con autoridad y responsabilidad final de especificar las políticas de certificado y asegurar que las prácticas y controles de la CA, cumplen totalmente las políticas de certificado respectivas. (Ver definición ampliada en el artículo 28 del Reglamento de la Ley N°8454).
Autoridad de registro RA (por sus siglas en inglés)	Entidad responsable de la identificación y autenticación de sujetos de certificados, que no es la CA y por lo tanto no firma ni emite certificados. Nota: Una RA puede ayudar en el proceso de solicitud del certificado, en el proceso de revocación o en ambos. La RA no necesita ser un organismo separado, sino que puede ser parte de la CA.
CA emisora	Autoridad certificadora registrada que forma parte de la jerarquía nacional de certificadores registrados, y que implementa una o varias políticas para emisión de certificados de usuario final.
CA de Políticas	Autoridad certificadora que forma parte de la raíz nacional, utilizada para segmentar el riesgo de acuerdo a la política de emisión para un tipo de certificado.
CA raíz	Autoridad certificadora registrada que se ubica en el ápice de la jerarquía nacional de certificadores registrados.
CA subordinada o Sub-CA	Autoridad certificadora registrada que está más abajo en relación a otra CA en la jerarquía nacional de certificadores registrados.
Calificador de la política	Información dependiente de la política, que acompaña un identificador de política de certificado en un certificado de la norma X.509.
Certificación	Proceso de creación de un certificado de llave pública para una entidad.
Certificado	La llave pública y la identidad de un suscriptor, junto con otra información, que se torna infalsificable al ser firmada con la llave privada de la autoridad certificadora que emitió ese certificado de llave pública.
Certificados de firma digital y autenticación de persona física en modalidad local	Proceso de creación de un certificado digital para una persona física de manera presencial.
Certificados de firma digital y autenticación de persona física en modalidad remota	Proceso de creación de un certificado digital para una persona física de manera no presencial.
Certificado suspendido	Suspensión de la validez de un certificado.
Compromiso	Violación de la seguridad de un sistema tal que pueda haber ocurrido una divulgación no autorizada de información sensible.
Comité asesor de políticas (CAP)	Ver “Autoridad de políticas (PA)”.
Control múltiple	Condición bajo la cual dos o más partes, mantienen por separado y confidencialmente, la custodia de componentes de una sola llave que, individualmente, no conlleva al conocimiento de la llave criptográfica resultante.
Datos de autenticación	Información utilizada para verificar la identidad afirmada de una entidad, tal como la de un individuo, un rol definido o una persona jurídica.

Términos	Definición
Datos de activación	Valores de los datos, distintos a las llaves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos (por ejemplo: por un PIN, una frase de paso o una llave mancomunada).
Declaración de divulgación PKI o PDS (por sus siglas en inglés)	Documento suplementario de una CP o una CPS que divulga la información crítica sobre las políticas y prácticas de una CA /PKI. Nota: Una declaración de divulgación PKI es un medio para divulgar y enfatizar la información normalmente cubierta en detalle por la CP y/o la CPS asociados. Por lo tanto, un PDS no tiene la intención de sustituir una CP o una CPS.
Declaración de prácticas de certificación o CPS (por sus siglas en inglés)	Declaración de las prácticas que emplea una autoridad certificadora al emitir certificados y que define el equipo, políticas y procedimientos que utiliza la CA para satisfacer los requisitos especificados en las políticas del certificado que son soportadas por esta.
Delta CRL	Partición del CRL dentro de una unidad de tiempo, que contiene los cambios realizados al CRL base desde su última actualización.
Diario de eventos o bitácora de auditoría	Registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.
Documento de identidad legalmente aceptado	Es el documento formal que, según el ordenamiento jurídico costarricense, sirve para identificar legalmente a un suscriptor. En el caso de las personas físicas costarricenses, es la cédula de identidad, para las personas físicas extranjeras, es el documento único de permanencia, según sea su estatus migratorio y para las personas jurídicas nacionales, la cédula de persona jurídica. En el caso de la cédula de persona jurídica el documento debe ser acompañado por una certificación de personería jurídica vigente (con menos de un mes de emitida), y el documento de identidad del representante legal.
Emisor del certificado	Organización cuyo nombre aparece en el campo del emisor de un certificado.
Cifrado	Proceso para convertir la información a un formato más seguro. En otras palabras, los datos que están en un formato claro, o sea entendible, se convierten mediante un proceso matemático a un formato cifrado o codificado, o sea ininteligible.
Entidad	CA, RA o entidad final.
Entidad final	Sujeto de certificado que utiliza su llave privada para otros propósitos diferentes al de firmar certificados. En este caso, puede tratarse de una persona física, un agente electrónico o una autoridad de sellado de tiempo.
Estampado de tiempo	Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.
Firma digital	Transformación criptográfica que, cuando está asociada a una unidad de datos, proporciona los servicios de autenticación del origen, integridad de los datos y no-repudio del firmante.
Firma digital certificada	Firma digital generada utilizando la llave privada correspondiente de un certificado de llave pública, emitido por una CA registrada.

Términos	Definición
Dispositivo criptográfico o módulo de seguridad de hardware (HSM por sus siglas en inglés)	Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.
Identificador de objeto u OID (por sus siglas en inglés)	Serie única de números enteros que identifica inequívocamente un objeto de información.
Infraestructura de llave pública o PKI (por sus siglas en inglés)	Estructura de *hardware*, *software*, recurso humano, procesos y políticas que utiliza tecnología de firma digital para facilitar una asociación comprobable entre el componente público de un par de llaves asimétricas con un suscriptor específico que posee la llave privada correspondiente. Nota La llave pública puede ser provista para verificación de firma digital, autenticación del sujeto en diálogos de comunicación, y/o para el intercambio o la negociación de llaves de encripción de mensajes.
Lista de revocación de certificados o CRL (por sus siglas en inglés)	Es una lista con los números de serie de los certificados que han sido revocados.
Parte que confía RP (por sus siglas en inglés)	Receptor de un certificado quien actúa confiando en ese certificado, en las firmas digitales verificadas usando ese certificado, o ambos.
Perfil del certificado	Especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).
Período de operación	Período de vigencia de un certificado que comienza en la fecha y la hora en que es emitido por una CA (o una fecha y una hora posterior, si se indica en el certificado) y termina en la fecha y la hora en que expira o se revoca el mismo.
Representante legal o representante con facultades suficientes	Quien ostente poder general o generalísimo en una persona jurídica.
Política de certificado o CP (por sus siglas en inglés)	Conjunto de reglas establecidas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.
Protocolo de consulta en línea del estado del certificado u OCSP (por sus siglas en inglés)	Protocolo para determinar el estado actual de un certificado en lugar de o como suplemento a la comprobación contra una CRL periódica, y que especifica los datos que necesitan ser intercambiados entre una aplicación que comprueba el estado de un certificado y el servidor que proporciona ese estado.
Re-emisión de llaves del certificado	Proceso por medio del cual una entidad con un par de llaves y un certificado recibe un nuevo certificado para una nueva llave pública, siguiendo la generación de un nuevo par de llaves.
Renovación del certificado	Proceso por medio del cual a una entidad le es emitida una nueva instancia de un certificado existente con un nuevo período de validez, conservando el mismo par de llaves.
Repositorio	Sistema para el almacenamiento y la distribución de los certificados y de la información relacionada (esto es, almacenamiento y recuperación de la política de certificado, estado del certificado, etc.).
Rol de confianza	Puesto de trabajo que realiza funciones críticas que, si se realiza insatisfactoriamente, puede tener un impacto adverso sobre el grado de confianza proporcionado por la CA.

Términos	Definición
Ruta de certificación	Secuencia ordenada de certificados de entidades que, junto con la llave pública de la entidad inicial en la ruta, pueden ser procesadas para obtener la llave pública de la entidad final en la ruta.
Servicios de validación del certificado	Servicios proporcionados por la CA o su agente quien realiza la tarea de confirmar la validez de un certificado a una parte que confía.
Sello electrónico	Firma digital certificada generada a partir de un certificado digital de sello electrónico de persona jurídica; se utilizan como parte de procesos automáticos de firma digital en donde, el dispositivo criptográfico que contiene las llaves asociadas al certificado, está activado para que pueda trabajar en forma desatendida y de esta manera no requiera de intervención humana a la hora de realizar cada firma digital.
Solicitud de certificado	Presentación a una CA por una RA (o a la CA raíz por una CA), su agente o un sujeto, de una solicitud de registro validada para registrar la llave pública del sujeto que se colocará en un certificado.
Solicitud de registro	Presentación por parte de una entidad a una RA (o CA) para registrar la llave pública de la entidad en un certificado.
Solicitud de servicio de validación	Petición realizada por la parte que confía a un servicio de validación para comprobar la validez de un certificado.
Sujeto	Entidad cuya llave pública es certificada en un certificado de llave pública.
Suscriptor	Entidad que se suscribe con una autoridad certificadora a nombre de uno o más sujetos.
Tramitador de certificados de persona jurídica	Persona física que es designada para actuar en representación de una persona jurídica, con el fin de solicitar y retirar en nombre de ésta los certificados de persona jurídica de sello electrónico y/o agente electrónico.
Validez del certificado	Aplicabilidad (apto para el uso previsto) y estado (activo, suspendido, revocado o expirado) de un certificado.
Verificación de la firma	Determinación y validación de: a) que la firma digital fue creada durante el período operacional de un certificado válido por la llave privada correspondiente a la llave pública que se encuentra en el certificado; b) que el mensaje no ha sido alterado desde que su firma digital fue creada.

Abreviaturas

Abreviatura	Descripción
CA	Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority).
CAP	Comité Asesor de Políticas.
CP	Políticas de Certificado (CP por sus siglas en inglés Certificate Policy).
CPS	Declaración de prácticas de Certificación (CPS por sus siglas en inglés Certifcation Practice Statement).
CRL	Listas de revocación de Certificados (CRL por sus siglas en inglés Certificate Revocation List).
DGD	Dirección de Gobernanza Digital.
DNS	Sistema de nombres de dominio (Domain name system).
ECA	Ente Costarricense de Acreditación.

Abreviatura	Descripción
FIPS	Estándar para los dispositivos criptográficos (FIPS por sus siglas en inglés Federal Information Processing Standard).
HSM	Dispositivo criptográfico (HSM por sus siglas en inglés Hardware Security Module).
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés International Standards Organization).
LGAP	Ley General de Administración Pública.
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.
NIC	Centro de información de redes de Internet en Costa Rica (NIC por sus siglas en inglés Network Information Center).
OCSP	Servicios de validación de certificados en línea (OCSP por sus siglas en inglés Online Certificate Status Protocol).
OEC	Organismo de Evaluación de la Conformidad.
OID	Identificador de Objeto (OID por sus siglas en inglés Object Identifier).
PDS	Declaración de divulgación PKI (PDS por sus siglas en inglés PKI Disclosure Statement).
PIN	Número de identificación Personal (PIN por sus siglas en inglés Personal Identification Number).
PKI	Infraestructura de llave pública (PKI por sus siglas en inglés Public Key Infraestructura).
RA	Autoridad de registro (RA por sus siglas en inglés Registration Authority).
RFC	Documento técnico aplicable que aún no es un estándar internacional (RFC por sus siglas en inglés Request for Comments).
RNP	Registro Nacional de Costa Rica.
TSA	Autoridad de estampado de tiempo (TSA por sus siglas en inglés Time Stamping Authority).
TSE	Tribunal Supremo de Elecciones.
URL	Localizador Uniforme de Recurso que permite asignar nombres a recursos en Internet (URL por sus siglas en inglés Uniform Resource Locutor).
UTC	Tiempo Universal Coordinado (UTC por sus siglas en inglés (Universal Time Coordinated).
X.509	Estándar utilizado para estructuras de datos y algoritmos de validación en las infraestructuras de llave pública.

2. Responsabilidades de publicación y del repositorio

2.1 Repositorios

Las autoridades emisoras son responsables de las funciones de repositorio para su propia CA. Las listas de los certificados emitidos a usuarios finales no se deben hacer públicas.
Sobre la revocación de certificados de suscriptores, las autoridades emisoras deben publicar el aviso de revocación de los certificados de sus suscriptores.

2.2 Publicación de información de certificación

La CA emisora debe mantener un repositorio basado en Web que permita a las partes que confían verificar en línea la revocación y cualquier otra información necesaria para validar el estado del certificado. La CA emisora debe proporcionar a las partes que confían la información de cómo encontrar el repositorio adecuado para verificar el estado del certificado y los servicios de validación de certificados en línea (OCSP) para la verificación en línea.
La CA emisora debe mantener publicada, entre otros aspectos, la versión actualizada de:

- La política de los certificados que implementa.

- La plantilla del acuerdo de suscriptor.
- Los certificados en la cadena de confianza.
- Las listas de revocación.

La CA Raíz, conserva el repositorio de certificados que contienen las cadenas de confianza y las listas de revocación, estas están publicadas en el sitio repositorio Web del MICITT, en la siguiente dirección:

- http://www.firmadigital.go.cr/

Esta CP, y la Información referente a la CA Raíz se mantiene publicada y actualizada en el sitio Web del MICITT, en la siguiente dirección:

- https://www.mifirmadigital.go.cr/

2.3 Tiempo o frecuencia de publicación

Las actualizaciones de las políticas de certificado se publicarán de acuerdo con lo establecido en la sección 9.12 de este documento. Las actualizaciones de acuerdos de suscriptores serán publicadas, cuando sufran modificaciones. La información de estados de certificado es publicada de acuerdo con las disposiciones de esta política, de acuerdo a la sección 4.9.7 de "Frecuencia de emisión de CRL".

2.4 Controles de acceso a los repositorios

La información publicada en el repositorio es información accesible únicamente para consulta. La CA emisora debe establecer controles para prevenir que personas no autorizadas agreguen, eliminen o modifiquen información de los repositorios

3. Identificación y autenticación

3.1 Nombres

3.1.1 Tipos de nombres

En la sección 3.1.4 se explican las reglas para interpretación del código de identificación, la que, en el caso de las personas físicas nacionales corresponde al número de cédula, para personas físicas extranjeras o diplomáticas, al número único de permanencia y para las personas jurídicas corresponde al número de cédula de persona jurídica. El uso del campo número de serie (serial number OID 2.5.4.5) se establece de acuerdo al RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile" como un atributo del nombre distintivo del sujeto.
A continuación, se presentan los formatos de los nombres para el suscriptor del certificado dependiendo de su tipo. Cuando los datos se encuentran en *itálica* significan que son valores de ejemplo.

En el caso de la CA Raíz:

Atributo	Valor	Descripción
Country (C)	CR	El código de país es asignado de acuerdo al estándar ISO 3166[3].
Organization (O)	MICITT	El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones es el responsable de la Raíz Nacional.

3 Norma ISO 3166 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países". Esta norma establece los códigos de dos caracteres para la asignación del país

Organization Unit (OU)	DCFD	La Dirección de Certificadores de Firma Digital.
Common Name	CA RAIZ NACIONAL – COSTA RICA	Nombre de la CA Raíz.
Serial Number {OID:2.5.4.5}	CPJ-2-100-098311	Número de cédula de persona jurídica en el Registro Nacional. El prefijo CPJ corresponde a Cédula Persona Jurídica.

En el caso de las CA de Políticas:

Atributo	Valor	Descripción
Country (C)	CR	El código de país es asignado de acuerdo al estándar ISO 3166.
Organization (O)	MICITT	El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones es el responsable de las CA de Políticas.
Organization Unit (OU)	DCFD	La Dirección de Certificadores de Firma Digital.
Common Name	CA POLITICA *PERSONA FISICA* – COSTA RICA	CA POLITICA + *Nombre de la política* – COSTA RICA
Serial Number {OID:2.5.4.5}	CPJ-2-100-098311	Número de cédula de persona jurídica en el Registro Nacional. El prefijo CPJ corresponde a Cédula Persona Jurídica.

En el caso de las CA emisoras:

Atributo	Valor	Descripción
Country (C)	CR	El código de país es asignado de acuerdo al estándar ISO 3166.
Organization (O)	*CORP. EJEMPLO S.A*[4]	Nombre de la empresa o institución definido en la certificación de personería jurídica.
Organization Unit (OU)	*CA EJEMPLO*	Unidad organizacional de la persona jurídica responsable de la CA emisora.
Common Name	CA *EJEMPLO - PERSONA FISICA*	CA + Nombre CA - Política. La Política puede ser: PERSONA FISICA, PERSONA JURÍDICA, SELLADO DE TIEMPO, u otra definida por la CA Raíz.
Serial Number {OID:2.5.4.5}	CPJ-*9-999-999999*	Número de cédula de persona jurídica en el Registro Nacional, debe ser validada durante el proceso de registro.

En el caso de suscriptor persona física:

Atributo	Valor	Descripción
Country (C)	CR	El código de país es asignado de acuerdo al estándar ISO 3166.
Organization (O)	*PERSONA FISICA*	La política identifica si se trata de un certificado para: Persona Física, Persona Jurídica o Sellado de Tiempo, o bien otra definida por la jerarquía

4 Los valores en itálica son colocados a manera de ejemplo.

		nacional de certificadores registrados.
Organization Unit (OU)	*CIUDADANO*	La clase de certificado es: CIUDADANO, EXTRANJERO o DIPLOMATICO.
Common Name	*JUAN PEREZ PEREZ* (*FIRMA*)	Nombre del suscriptor, según documento de identificación oficial, en mayúsculas y sin tildes El propósito debe ser FIRMA o AUTENTICACION.
Serial Number {OID:2.5.4.5}	CPF-*01-0449-0161*	El formato del documento de identificación se especifica en la sección 3.1.4 "Reglas para la interpretación de varias formas de nombres".
Surname (SN) {OID:2.5.4.4}	*PEREZ PEREZ*	Se registran los dos apellidos del suscriptor, en mayúsculas y sin tildes.
GivenName (G) {OID:2.5.4.42}	*JUAN*	Se registra el nombre del suscriptor, en mayúsculas y sin tildes.

En el caso de suscriptor para persona jurídica:

Atributo	Valor	Descripción
Country (C)	CR	El código de país es asignado de acuerdo al estándar ISO 3166.
Organization (O)	*PERSONA JURÍDICA*	La política identifica si se trata de un certificado para: Persona Física, Persona Jurídica o Sellado de Tiempo, o bien otra definida por la jerarquía nacional de certificadores registrados.
Organization Unit (OU)		Identificador opcional para unidades organizacionales vinculadas jurídicamente a la persona jurídica solicitante.
Common Name	*CORTE SUPREMA DE JUSTICIA (SELLO ELECTRONICO)*	Razón social/Nombre de la persona jurídica que solicita el certificado, según la información del Registro de Personas Jurídicas de Registro Nacional. El propósito debe ser SELLO ELECTRÓNICO o AGENTE ELECTRÓNICO. Para el caso de entidades con personería jurídica instrumental puede indicarse en este campo el nombre de la entidad que la utiliza, indicando en el campo OU el nombre de la persona jurídica titular del número de cédula jurídica compartido.
Serial Number {OID:2.5.4.5}	CPJ-*2-300-042155*	El formato de la cédula de persona jurídica se especifica en la sección 3.1.4 "Reglas para la interpretación de varias formas de nombres".
Subject Alternative Name {OID:2.5.29.17}	Dns=www.poder-judicial.go.cr	Valor opcional donde se coloca el nombre del dominio, y aplica únicamente para los certificados de AGENTE ELECTRÓNICO.

En el caso de suscriptor para autoridad de sellado de tiempo:

Atributo	Valor	Descripción
Country (C)	CR	El código de país es asignado de acuerdo al estándar ISO 3166.
Organization (O)	*LABORATORIO COSTARRICENSE DE METROLOGIA*	Nombre de la empresa o institución que solicita el certificado.

Organization Unit (OU)	*0001*	Identificador consecutivo para la autoridad de sellado de tiempo. Este campo es responsabilidad de la empresa o institución proporcionarlo, y es utilizado para mantener la continuidad del negocio.
Common Name	TSA *LABORATORIO COSTARRICENSE DE METROLOGIA*	TSA + *Nombre de la persona jurídica*, según la información del Registro de Personas Jurídicas de Registro Nacional. Se concatena el propósito de TSA (Time Stamping Authority) para indicar que es una autoridad de sellado de tiempo.
Serial Number {OID:2.5.4.5}	CPJ-3-007-351220	El formato de la cédula de persona jurídica se especifica en la sección 3.1.4 "Reglas para la interpretación de varias formas de nombres".

3.1.2 Necesidad de nombres significativos

El nombre significativo corresponde al nombre especificado en el documento oficial presentado por el solicitante en el momento de registro. Además, para evitar errores de interpretación en el nombre de personas físicas, se registra el nombre y los apellidos en atributos separados (GivenName y SurName, respectivamente).

3.1.3 Anonimato o pseudónimos de los suscriptores

De acuerdo con la Ley N°8454, "Ley de certificados, firmas digitales y documentos electrónicos" y su reglamento, los certificados de firma digital no admiten anonimato para cumplir con el requisito de "No Repudio". El pseudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del certificado.

3.1.4 Reglas para la interpretación de varias formas de nombres

Certificados de CA emisora
La cédula de persona jurídica es definida por el Registro de Personas Jurídicas de Registro Nacional y debe cumplir el siguiente formato:

Tipo de documento	Prefijo	Formato
Cédula de persona jurídica	CPJ	CPJ-9-999-999999

Certificados de firma digital y autenticación de persona física
El nombre común tiene concatenado el propósito del certificado entre paréntesis, el cual puede ser únicamente uno de los siguientes:

- (FIRMA)
- (AUTENTICACION)

El número de cédula de persona física y el número único de permanencia deben cumplir el siguiente formato:

Tipo de documento	Prefijo	Formato
Cédula de persona física	CPF	CPF-99-9999-9999
Número único de permanencia	NUP	NUP-9XXX99999999[5]

5 El número único de permanencia (NUP) está conformado por los siguientes elementos:

- Código de No Nacional, es un dígito, y siempre se asignan los números 1 o 5.

Certificados de sello electrónico y agente electrónico de persona jurídica y de autoridad de sellado de tiempo

La cédula de persona jurídica debe cumplir el siguiente formato:

Tipo de documento	Prefijo	Formato
Cédula de persona jurídica	CPJ	CPJ-9-999-999999

3.1.5 Unicidad de los nombres

Para cada suscriptor, la CA emisora debe asegurar que el "nombre distintivo del suscriptor" (*subject distinguished name*) es único dentro de la jerarquía nacional de certificadores registrados, a través de una verificación dentro del proceso de inscripción.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas

La jerarquía nacional de certificadores registrados no arbitrará, mediará o resolverá ninguna disputa concerniente a la propiedad de nombres de dominio, nombres de empresas, instituciones o personas jurídicas, o marcas registradas.

3.2 Validación inicial de identidad

3.2.1 Método para probar posesión de la llave privada

El solicitante del certificado debe demostrar que posee la llave privada correspondiente a la llave pública que estará en lista en el certificado, utilizando los mecanismos que para estos efectos le provean la CA o la RA.

El método de prueba de posesión de la llave privada puede ser el PKCS#10, u otras demostraciones criptográficas equivalentes, aprobadas por la DGD.

3.2.2 Autenticación de identidad de persona jurídica

La identidad de la persona jurídica solicitante debe ser confirmada por la CA emisora, o por la RA, donde aplique, de acuerdo con los procedimientos establecidos. Como mínimo, se debe verificar el nombre o razón social, la cédula de persona jurídica y representante legal debidamente acreditado contra las bases de datos oficiales correspondientes.
En el caso de los certificados de persona jurídica, si el solicitante requiere incluir información en el campo "unidad organizacional" (Organization Unit), la CA emisora, o donde aplique, la RA, deberá solicitar toda la información necesaria al suscriptor para garantizar el vínculo jurídico entre la unidad organizacional en cuestión y la persona jurídica solicitante.
En el caso de los certificados de agente electrónico de persona jurídica, si el solicitante requiere incluir uno o más nombres DNS en el campo "nombre alternativo del sujeto" (Subject Alternative Name, o también conocido como SAN por sus siglas en inglés), la CA emisora, o donde aplique, la RA, debe verificar la información de DNS suministrada por el solicitante, contra los datos oficiales correspondientes.

- Código de país, es un código alfanumérico de acuerdo con el ISO-3166 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países." con formato de 3 letras, por ejemplo: NIC = Nicaragua, CRI = Costa Rica, USA = Estados Unidos de América, COL= Colombia, etc.
- Consecutivo por país, corresponde a la numeración de seis dígitos, que representa la cantidad de personas que han ingresado con estatus migratorio al país en el momento de la inscripción.
- Dígitos de verificación, son dos dígitos que verifican la consistencia de la notación para ese extranjero.

3.2.3 Autenticación de identidad de persona física

Para la identificación de la persona física la CA emisora o RA deberá realizar la verificación de la identidad suministrada por el solicitante, confirmando la validez y vigencia del documento legalmente aceptado, presentado por el solicitante. Este proceso debe realizarse cumpliendo con los siguiente:

a) En presencia física de la persona (cara a cara), o
b) Mediante una autorización electrónica firmada con un certificado de firma digital certificada expedido conforme con el numeral a) del punto 3.2.3, o
c) Utilizando los servicios de verificación de identidad oficiales de las autoridades competentes (proveedores de identidad) que certifiquen una seguridad equivalente en términos de fiabilidad a la presencia física.

La CA emisora, o donde aplique, la RA, debe verificar la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.4 Información del suscriptor no verificada

No aplica, la información incluida en el certificado es verificada durante el proceso de autenticación de la identidad.

3.2.5 Validación de la Autoridad

La CA emisora, o donde aplique, la RA, debe validar la autoridad que posee el solicitante para gestionar un tipo de certificado específico. Además, debe validar que el solicitante no posea impedimentos legales de acuerdo con la información oficial vigente para tales efectos.
En el caso de certificados de persona física, debe validar que sea mayor de edad.
En el caso de certificados de persona jurídica, debe validarse que sea un representante legal o un representante con facultades suficientes para hacer la solicitud de los certificados.
La CA emisora, o donde aplique, la RA, debe verificar la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.6 Criterios para interoperabilidad

Se debe garantizar la interoperabilidad de los certificados emitidos, siempre y cuando la CA emisora cumpla con la política de la raíz y estén adscritas a la jerarquía nacional de certificadores registrados. La homologación de certificados extranjeros se hará de acuerdo con el marco normativo vigente y los procedimientos establecidos por la DGD para tales casos.

3.3 Identificación y autenticación para solicitudes de re-emisión de llaves

3.3.1 Identificación y autenticación para re-emisión de llaves rutinaria

No se permite la re-emisión de certificados. En dado caso, se debe optar por un nuevo certificado.

3.3.2 Identificación y autenticación para la re-emisión de llaves después de una revocación

Bajo estas circunstancias la re-emisión de llaves no aplica.

3.4 Identificación y autenticación para solicitudes de revocación

Los procedimientos de revocación deben asegurar, previo a cualquier revocación, que la solicitud de revocación ha sido generada por el suscriptor del certificado o por una entidad autorizada para tales propósitos.
Los procedimientos aceptados para la autenticación de solicitudes de revocación presentadas por el suscriptor incluyen alguno de los siguientes medios:

- La recepción de un mensaje firmado digitalmente por el suscriptor del certificado.
- Mediante la utilización de un mecanismo de verificación previamente definido para autorizar el proceso de revocación, por ejemplo, comprobación de una frase de desafío, comprobación de preguntas de seguridad, confirmación de correo electrónico, segundo factor de autenticación, entre otras.
- Presencialmente, a través de los procesos de autenticación de identidad (secciones 3.2.2 y 3.2.3).
- Cualquier otro medio aprobado por la DGD que permita una autenticación robusta.

Los procedimientos aceptados para la autenticación de solicitudes de revocación presentadas por una entidad autorizada para tales efectos (ver sección 4.9.2), incluye la recepción de un mensaje firmado por una autoridad competente.

4. Requerimientos operacionales del ciclo de vida del certificadoSolicitud de certificado

4.1.1 Quién puede presentar una solicitud de certificado

En la siguiente lista se detallan las personas que pueden presentar una solicitud de certificado:

- Para el caso de certificados de CA de políticas, el Director de Certificadores de Firma Digital.
- Para el caso de certificados de CA emisoras, el representante legal o apoderado con poderes suficientes de la entidad a ser registrada.
- Para el caso de certificados de autenticación y de firma digital de persona física, cualquier persona mayor de edad que cuente con un documento de identidad legalmente aceptado y vigente, incluyendo una firma digital certificada vigente y emitida con las disposiciones de esta CP, que será el sujeto a cuyo nombre se emita el certificado.
- Para el caso de certificados de sello electrónico y agente electrónico de persona jurídica, el representante legal o representante con facultades suficientes de la persona jurídica a la que representa (por ejemplo un tramitador de certificados digitales de persona jurídica debidamente registrado ante la Autoridad Certificadora).
- Para los certificados de Autoridad de Sellado de Tiempo, el representante legal o apoderado con poderes suficientes de la entidad de sellado de tiempo (TSA).

4.1.2 Proceso de inscripción y responsabilidades

Durante el proceso de inscripción, el solicitante debe firmar un acuerdo de suscriptor, donde se establecen las responsabilidades y deberes asumidos con el uso del certificado.
La DGD tiene la responsabilidad de:

- Ejecutar el proceso de registro y verificación de identidad de las CA emisoras.
- Velar porque la entidad solicitante cumpla los requisitos establecidos en la Ley N°8454, Ley de certificados, firmas digitales y documentos electrónicos y su reglamento.
- Informar al suscriptor de sus deberes y responsabilidades con respecto al uso del certificado.
- Emitir el certificado de acuerdo con la información suministrada en la solicitud de certificado.

La CA emisora tiene la responsabilidad de:

- Validar la identidad de la RA que remite las solicitudes.
- Validar la información suministrada en la solicitud.
- Emitir el certificado de acuerdo con la información suministrada en la solicitud.
- Enviar el certificado a la RA para que sea entregado al suscriptor.

La RA tiene la responsabilidad de:

- Ejecutar el proceso de registro y verificación de identidad y de las facultades del solicitante para solicitar un determinado certificado dependiendo del tipo de certificado.
- Remitir la solicitud de certificado digital a la CA emisora, firmada digitalmente.
- Informar al suscriptor de sus deberes y responsabilidades con respecto al uso del certificado.

El solicitante tiene las siguientes responsabilidades dependiendo del tipo de certificado:

Certificados de CA emisora

- Completar el formulario de inscripción de certificado y proveer información correcta y verdadera. Esta información debe presentarse ante la RA, para este caso la DGD.
- Presentar un documento de identificación legalmente aceptado y vigente, así como una personería jurídica vigente (con menos de un mes de emitida) donde se establezca su relación como representante legal o apoderado con poderes suficientes de la empresa o institución a certificar.
- Generar la solicitud de certificado de forma que se demuestre la posesión de la llave privada correspondiente a la llave pública entregada, cumpliendo lo estipulado en el apartado 3.2.1.
- Firmar el acuerdo de suscriptor.

Certificados de firma digital y autenticación de persona física

- Completar el formulario de inscripción de certificado y proveer información correcta y verdadera.
- Presentar un documento de identificación legalmente aceptado y vigente, o firmar digitalmente una autorización utilizando firma digital certificada vigente y emitida con las disposiciones de esta CP.
- Mediante la utilización de un mecanismo de verificación previamente definido para autorizar el proceso de revocación, por ejemplo, comprobación de una frase de desafío, comprobación de preguntas de seguridad, confirmación de correo electrónico, segundo factor de autenticación, entre otras.
- Generar la solicitud de certificado de forma que se demuestre la posesión de la llave privada correspondiente a la llave pública entregada, cumpliendo con lo dispuesto en el apartado 3.2.1.
- Firmar el acuerdo de suscriptor.

Certificados de sello electrónico y agente electrónico de persona jurídica

- Completar el formulario de inscripción de certificados y proveer información correcta y verdadera.
- Presentar un documento de identificación legalmente aceptado y vigente, así como una personería jurídica con menos de un mes de emitida, o los documentos legales

suficientes que garanticen su relación como representante legal o representante con facultades suficientes de la persona jurídica solicitante. Para los certificados de agente electrónico, en el caso de requerir que uno o varios nombres DNS formen parte del campo nombre alternativo del sujeto (Subject Alternative Name o SAN por sus siglas en inglés) es necesario que el representante legal o representante con facultades suficientes de la persona jurídica solicitante, presente evidencia de que el nombre de dominio solicitado está registrado o gestionado a nombre de la persona jurídica que representa (ver sección 7.1.2.3)

- Cuando aplique, generar la solicitud de certificado cumpliendo con el apartado 3.2.1 de esta CP y presentarla ante la CA, con lo que se demuestra la posesión de la llave privada correspondiente a la llave pública entregada.
- Firmar el acuerdo de suscriptor.

Certificados de Autoridad de Sellado de Tiempo (TSA)

- Completar el formulario de inscripción de certificado y proveer información correcta y verdadera ante la DGD.
- Cumplir con todas las responsabilidades señaladas anteriormente para solicitante de certificados de sello electrónico y agente electrónico de persona jurídica.

4.2 Procesamiento de la solicitud de certificado

4.2.1 Ejecución de las funciones de identificación y autenticación

Certificados de CA emisora y de autoridad de sellado de tiempo
La encargada de estas funciones es la DGD, entidad que debe velar por el cumplimiento de la identificación y la autenticación de acuerdo con las disposiciones establecidas en la sección 3.2.

Certificados de firma digital y autenticación de persona física o certificados de sello electrónico y agente electrónico de persona jurídica
La encargada de estas funciones es la autoridad de registro (RA), o donde aplique la CA, que debe velar por el cumplimiento de la identificación y la autenticación de acuerdo con las disposiciones establecidas en la sección 3.2.

4.2.2 Aprobación o rechazo de solicitudes de certificado

Certificados de CA emisora y de autoridad de sellado de tiempo (TSA)
La DGD debe administrar y supervisar el proceso de certificación, en particular lo concerniente a la aceptación o rechazo de las aplicaciones para certificados de autoridad certificadora.
Para optar por un certificado de autoridad certificadora, la CA solicitante debe cumplir con todos los requisitos establecidos en la Ley N°8454, su Reglamento y demás lineamientos establecidos por la DGD.

Certificados de firma digital y autenticación de persona física o certificados de sello electrónico y agente electrónico de persona jurídica
La RA debe rechazar cualquier solicitud de certificado que no cumpla con la Ley, su Reglamento y demás lineamientos establecidos por la DGD. Asimismo, la CA emisora debe rechazar cualquier solicitud proveniente de una RA que no cumpla con los requisitos para la emisión del certificado.

4.2.3 Tiempo para procesar solicitudes de certificado

El tiempo de procesamiento de solicitudes de certificados (tiempo entre la solicitud emitida a la CA y la emisión del certificado al suscriptor) de persona física, cuando el proceso se realice en forma automática, no debe ser mayor a diez minutos.

En cualquier otro caso, las CA y RA procesarán las solicitudes de certificados dentro de un tiempo razonable, a menos que se especifiquen otros parámetros en el acuerdo de suscriptor, en la CPS o en otros acuerdos entre los participantes.

4.3 Emisión de certificado

4.3.1 Acciones de la CA durante la emisión de certificados

Certificados de CA y certificados de autoridad de sellado de tiempo (TSA)
La CA debe verificar que el solicitante cumple con los requisitos de esta política, con las normas técnicas y con la legislación aplicable.

Certificados de firma digital y autenticación de persona física o certificados de sello electrónico y agente electrónico de persona jurídica
La CA debe verificar que las solicitudes de certificado provengan de RAs autorizadas. Una vez creado el certificado, la CA debe remitirlo a la RA desde la cual ingresó la solicitud.

4.3.2 Notificación al suscriptor por parte de la CA sobre la emisión del certificado

Certificados de CA emisora y certificados de autoridad de sellado de tiempo (TSA)
La DGD debe notificar a la CA emisora o la TSA solicitante sobre la emisión del certificado, de acuerdo a los procedimientos definidos para tales efectos.

Certificados de firma digital y autenticación de persona física
La CA emisora deberá notificar a la RA y directamente al suscriptor, la emisión del nuevo certificado de forma inmediata.

Certificados de sello electrónico y agente electrónico de persona jurídica
Cuando las circunstancias lo permitan, la RA, o donde aplique la CA, entregará los certificados en forma presencial, en cuyo caso la notificación será inmediata. En cualquier otro caso, la notificación se realizará de acuerdo a los procedimientos definidos para tales efectos.

4.4 Aceptación de certificado

4.4.1 Conducta constitutiva de aceptación de certificado

Certificados de CA emisora y certificados de autoridad de sellado de tiempo (TSA)
El proceso de instalación del certificado respectivo por parte de la CA emisora o TSA solicitante, constituirá la aceptación del certificado.

Certificados de firma digital y autenticación de persona física
El certificado se da por aceptado cuando la persona firma digitalmente un comprobante de aceptación del certificado entregado, esta es la primera vez que se usa y permite al suscriptor verificar que el certificado está funcionando correctamente.

Certificados de sello electrónico y agente electrónico de persona jurídica
El proceso de instalación de los certificados respectivos por parte de la persona jurídica que utiliza los certificados, constituirá la aceptación de los certificados.

4.4.2 Publicación del certificado por la CA

La CA no debe publicar información de los certificados emitidos en los repositorios de acceso público.

4.4.3 Notificación de la emisión del certificado por la CA a otras entidades

No se definen entidades externas que necesiten o requieran ser notificadas acerca de los certificados emitidos por las CA.

4.5 Uso del par de llaves y del certificado

4.5.1 Uso de la llave privada y del certificado por el suscriptor

El uso de la llave privada correspondiente a la llave pública contenida en el certificado solamente debe ser permitido una vez que el suscriptor haya aceptado el certificado emitido. Dicho uso debe realizarse en concordancia con la normativa aplicable, lo estipulado en este CP, y los contratos de suscriptor respectivos.
Los suscriptores deben proteger sus llaves privadas del uso no autorizado y deben descontinuar su uso después de la expiración o revocación del certificado.

Certificados de CA

- CA raíz: la llave privada sólo puede ser utilizada para firmar certificados de CA de políticas.
- CA políticas: Las CA de políticas son CA emisoras cuya llave privada únicamente puede ser utilizada para firmar certificados de CA emisoras subordinadas (SubCa) y autoridades certificadoras de sellado de tiempo.
- CA emisora de persona física o persona jurídica: la llave privada solo debe ser utilizada para firmar certificados de autenticación y firma digital de personas físicas o certificados de sello electrónico y agente electrónico de personas jurídicas.

Certificados de firma digital y autenticación de persona física
El uso que se le dé a los certificados de persona física debe ser acorde con lo dispuesto en la sección 6.1.7.

Certificados de sello electrónico de persona jurídica
Los certificados de sello electrónico serán utilizados para actos de la persona jurídica suscriptora, salvo aquellos casos donde se determine su inadmisibilidad legal o administrativa. Dichos actos generan responsabilidad de conformidad con el Artículo 10 de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N°8454. [6]
Cada persona jurídica deberá desarrollar y establecer los mecanismos de seguridad informática y de infraestructura física, así como los reglamentos, procedimientos o políticas que considere pertinentes para resguardar y delimitar el uso de dicho certificado en su organización.
Las personas jurídicas que hagan uso de los certificados de sello electrónico deberán proveer las herramientas necesarias y adecuadas para que tanto los ciudadanos como otras administraciones puedan verificar la validez de sus sellos electrónicos.
Cada persona jurídica decidirá sobre y será responsable del mecanismo que desee utilizar para la gestión de las llaves privadas que permiten el uso de sus certificados de persona jurídica, según sus políticas de seguridad y control interno.
Con respecto a la utilización de las llaves, el uso que se le dé a los certificados de sello electrónico debe ser acorde con lo dispuesto la sección 6.1.7.

Certificados de agente electrónico de persona jurídica
Cada persona jurídica deberá desarrollar y establecer los mecanismos de seguridad informática y de infraestructura física, así como los reglamentos, procedimientos o políticas que considere pertinentes para resguardar y delimitar el uso de dicho certificado en su organización.
Cada persona jurídica decidirá sobre y será responsable del mecanismo que desee utilizar para la gestión de las llaves privadas que permiten el uso de sus certificados de persona jurídica, según sus políticas de seguridad y control interno.

---

6 Artículo 10.- Presunción de autoría y responsabilidad

Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.

Con respecto a la utilización de las llaves, el uso que se le dé a los certificados de agente electrónico debe ser acorde con lo dispuesto la sección 6.1.7.

Certificados autoridad de sellado de tiempo (TSA)
La llave privada solo debe ser utilizada para prestar el servicio de sellado de tiempo.

4.5.2 Uso de la llave pública y del certificado por la parte que confía

Las partes que confían deben aceptar las estipulaciones establecidas en este CP, en lo que les resulte aplicable, como condición indispensable para confiar en el certificado.
La confianza en un certificado debe ser razonable, de acuerdo con las circunstancias. Si las circunstancias indican la necesidad de verificaciones adicionales, la parte que confía debe obtener tales verificaciones para que la confianza sea considerada razonable.
Antes de cualquier acto de confianza las partes que confían deben evaluar en forma independientemente:

- La pertinencia del uso del certificado para cualquier propósito dado y determinar que la voluntad del certificado, de hecho, sea utilizada para un propósito apropiado que no está prohibido o de otra forma restringido por este CP. Las CA o RA no son responsables por la evaluación de la pertinencia en el uso de un certificado.
- Que el certificado sea utilizado de acuerdo con las disposiciones de esta CP (por ejemplo: Si en el certificado faltan los propósitos de firma y no repudio en el atributo de KeyUsage, entonces el certificado no puede ser confiable para validar la firma de un suscriptor).
- El estado del certificado y el estado de todos los certificados de las CA en la cadena que emitieron el certificado. Si cualquiera de los certificados en la cadena del certificado ha sido revocado, la parte que confía es la única responsable de investigar si la confianza en una firma digital efectuada por un suscriptor antes de la revocación de un certificado en la cadena es razonable. Cualquier confianza de este tipo es asumida únicamente bajo el riesgo de la parte que confía.

Si se determina que el uso del certificado es apropiado, las partes que confían deben utilizar el hardware y software necesario para ejecutar la verificación de la firma digital u otra operación criptográfica que ellos deseen efectuar, como una condición para confiar en los certificados relacionados con tales operaciones.

4.6 Renovación de certificado

La renovación del certificado no está permitida por esta CP, cuando un certificado requiera ser renovado debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de este CP.

4.6.1 Circunstancias para renovación de certificado

No aplica.

4.6.2 Quién puede solicitar renovación

No aplica.

4.6.3 Procesamiento de solicitudes de renovación de certificado

No aplica.

4.6.4 Notificación al suscriptor sobre la emisión de un nuevo certificado

No aplica.

4.6.5 Conducta constitutiva de aceptación de un certificado renovado

No aplica.

4.6.6 Publicación por la CA del certificado renovado

No aplica.

4.6.7 Notificación por la CA de la emisión de un certificado a otras entidades

No aplica.

4.7 Re-emisión de llaves de certificado

La re-emisión del certificado no está permitida por esta CP, cuando un certificado requiera ser re-emitido debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de este CP.

4.7.1 Circunstancia para re-emisión de llaves de certificado

No aplica.

4.7.2 Quién puede solicitar la certificación de una nueva llave pública

No aplica.

4.7.3 Procesamiento de solicitudes de re-emisión de llaves de certificado

No aplica.

4.7.4 Notificación al suscriptor sobre la reemisión de un nuevo certificado

No aplica.

4.7.5 Conducta constitutiva de aceptación de un certificado reemitido

No aplica.

4.7.6 Publicación por la CA de los certificados reemitidos

No aplica.

4.7.7 Notificación por la CA de la reemisión de un certificado a otras entidades

No aplica.

4.8 Modificación de certificados

4.8.1 Circunstancias para modificación del certificado

Cuando se requiera la modificación de la información contenida en un certificado debe revocarse y realizar una solicitud para un nuevo certificado, de acuerdo con la sección 4.1.

4.8.2 Quién puede solicitar modificación del certificado

No aplica.

4.8.3 Procesamiento de solicitudes de modificación del certificado

No aplica.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

No aplica.

4.8.5 Conducta constitutiva de aceptación del certificado modificado

No aplica.

4.8.6 Publicación por la CA de los certificados modificados

No aplica.

4.8.7 Notificación por la CA de emisión de certificado a otras entidades

No aplica.

4.9 Revocación y suspensión de certificado

4.9.1 Circunstancias para la revocación

Certificados de CA:

- A petición de la CA que considera o sospecha que su llave privada fue comprometida.
- Identificación o componentes de afiliación inválidos.
- Violación del acuerdo de suscriptor.
- Insolvencia, cese de actividades, quiebra o liquidación de la CA.
- Se comprueba la expedición de certificados falsos.
- Reincidencia en cualquiera de las infracciones que le hayan merecido una sanción de suspensión, dentro de los cinco años siguientes.
- Cuando se tienen razones para creer que el certificado no fue emitido de acuerdo a los lineamientos de la CP aplicable.
- Cuando se determina que los pre-requisitos para la emisión del certificado no fueron satisfechos.

Certificados de firma digital y autenticación de persona física, de sello electrónico y agente electrónico de persona jurídica, y de sellado de tiempo:

- A petición del suscriptor, a favor de quién se expidió, quién tiene razones o sospechas para creer que su llave privada ha sido comprometida.
- Cuando se confirme, por medio del procedimiento definido por la CA, que el suscriptor ha comprometido su confiabilidad, desatendiendo los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido otra información relevante, con el propósito de obtener o re-emitir el certificado. La CA deberá notificar a la persona.
- Por fallecimiento (en el caso de persona física), ausencia legalmente declarada, interdicción o insolvencia.
- Cuando el suscriptor finaliza el contrato por voluntad propia.
- Por errores de información del certificado, por ejemplo el nombre del suscriptor o alguno de los atributos.
- El acuerdo entre el suscriptor y la CA emisora se ha terminado.
- Cuando se tienen razones para creer que el certificado no fue emitido de acuerdo a los lineamientos de la CP aplicable.
- Cuando se determina que los pre-requisitos para la emisión del certificado no fueron satisfechos.
- Cuando la información incluida dentro del certificado es incorrecta o ha cambiado.
- Para el caso de los certificados de persona jurídica, cuando venza el plazo social de la persona jurídica o cuando la misma sea disuelta.

Adicionalmente, cuando se determine que el uso del certificado atenta contra la seguridad del Sistema Nacional de Certificación Digital. Esto se determinará con base en la legislación aplicable,

la naturaleza y el número de denuncias recibidas, la identidad del denunciante, y cualquier otra que la DGD determine.

4.9.2 Quién puede solicitar revocación

De pleno derecho el suscriptor del certificado puede solicitar la revocación de su certificado, ya sea por voluntad propia o por compromiso de su llave privada. En caso de sospecha o compromiso de su llave privada, la notificación debe realizarla en forma inmediata a la CA correspondiente.
Para todos los casos, la CA emisora del certificado y la autoridad judicial competente pueden solicitar la revocación del certificado.
Asimismo, pueden solicitar la revocación los siguientes participantes según el tipo de certificado:

Para certificados de CA emisora o TSA

- El representante legal o apoderado con poderes suficientes de la CA emisora o TSA.
- La DGD.

Para certificados de firma digital y autenticación de persona física

- El Tribunal Supremo de Elecciones, en caso de fallecimiento.

Para certificados de sello electrónico y agente electrónico de persona jurídica

- El representante legal o representante con facultades suficientes de la persona jurídica suscriptora del certificado (por ejemplo, el tramitador de certificados digitales de persona jurídica vigente y debidamente registrado ante la Autoridad Certificadora).
- El Registro Nacional, por medio de su registro de personas jurídicas.

Además, cualquier persona puede solicitar la revocación de un certificado ante la CA correspondiente presentando evidencia contundente que revele el compromiso de la llave privada del suscriptor.

4.9.3 Procedimiento para la solicitud de revocación

Verificar que la solicitud de revocación ha sido presentada por el suscriptor del certificado o por una autoridad competente, de acuerdo con la sección 3.4.
Las solicitudes para la revocación de certificados de CA emisoras deben ser autenticadas por sus entidades superiores dentro de la jerarquía nacional de certificadores registrados, para asegurar que la revocación de una CA emisora ha sido solicitada por una entidad autorizada para tales efectos.
Para los casos donde un suscriptor posea dos o más certificados vigentes del mismo tipo y propósito, la CA emisora tendrá la responsabilidad de brindar al suscriptor la información suficiente que le permita determinar con exactitud cuál de los certificados es el que dicho suscriptor desea revocar, así como de informarle al momento de la revocación del estado de sus otros certificados vigentes.

4.9.4 Periodo de gracia para solicitud de revocación

No se estipulan periodos de gracia para revocación de certificados, salvo los impuestos por la Ley para realizar apelaciones.

4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación

Las solicitudes de revocación deben ser procesadas en un rango de tiempo razonable, de acuerdo con el procedimiento para la solicitud de revocación (ver sección 4.9.3). Cuando la solicitud provenga del suscriptor y se utilicen mecanismos electrónicos automatizados, la revocación debe realizarse en forma inmediata.

4.9.6 Requerimientos de verificación de revocación para las partes que confían

Las partes que confían deben evaluar el estado del certificado y el estado de todos los certificados de las CA en la cadena a la que pertenece el certificado, antes de confiar en él.
En caso de que cualquiera de los certificados en la cadena del certificado haya sido revocado, la parte que confía es la única responsable de investigar si la confianza en una firma digital efectuada por un suscriptor antes de la revocación de un certificado en la cadena es razonable. Cualquier confianza de este tipo es asumida únicamente bajo el riesgo de la parte que confía. Para estos propósitos las partes que confían pueden verificar el estado del certificado mediante el servicio de OCSP o la lista de revocación más reciente, de acuerdo con su grado de tolerancia al riesgo.

4.9.7 Frecuencia de emisión de CRL

CA Raíz
La CA Raíz debe actualizar su lista de revocación cada cuatro meses y en caso de darse una revocación del certificado de una CA de Políticas se debe actualizar de forma inmediata, en cuyo caso se debe notificar a las CA subsecuentes.

CA de Políticas
La CA de Políticas debe actualizar su lista de revocación cada dos meses y cada vez que se presente una revocación del certificado de una CA emisora, en cuyo caso se debe notificar a todas las CA emisoras.

CA emisora
La CA emisora debe actualizar y publicar las listas de revocación al menos una vez a la semana. Además deberá publicar los Delta CRL una vez al día.

4.9.8 Latencia máxima para CRLs

La CA o TSA debe publicar la CRL en el repositorio en un plazo no mayor a dos horas posterior a su generación.

4.9.9 Disponibilidad de verificación de revocación/estado en línea

Todas las CA o TSA deben mantener disponible un repositorio con información del estado de los certificados emitidos por ésta, el cual puede ser accedido vía Web. Adicionalmente, para la CA emisora registrada es obligatorio implementar el servicio de validación en línea OCSP.

4.9.10 Requerimientos para verificar la revocación en línea

La parte que confía debe verificar el estado de un certificado en el cual desea confiar, utilizando los mecanismos de verificación del estado de certificados establecidos en la sección anterior.

4.9.11 Otras formas de advertencias de revocación disponibles

No se estipulan.

4.9.12 Requerimientos especiales por compromiso de llaves reemitidas

La DGD debe notificar en el menor tiempo posible a todos los participantes de la jerarquía nacional de certificadores registrados acerca del compromiso de la llave privada de alguna de las CA.

4.9.13 Circunstancias para suspensión

4.9.13.1 Suspensión de certificados para personas físicas o certificados para de personas jurídicas

De conformidad con el artículo 14 de la Ley N°8454 de certificados digitales, las circunstancias de suspensión son:

a. Por petición del propio usuario a favor de quién se expidió el certificado.
b. Como medida cautelar, cuando el certificador que lo emitió tenga sospechas fundadas de que el propio usuario haya comprometido su confiabilidad, para obtener el certificado.
c. Si contra el usuario se ha dictado auto de apertura a juicio, por delitos en cuya comisión se haya utilizado la firma digital.
d. Por no cancelar oportunamente el costo del servicio.

Para los efectos prácticos se puede implementar la suspensión de certificados de personas físicas o de personas jurídicas, como la anulación técnica del certificado, que evite que pueda seguir siendo utilizado para el propósito de firma por parte del suscriptor. Además, ninguna CA emisora podrá expedirle un certificado de firma o sello electrónico mientras el estado de suspensión se encuentre vigente. Este aspecto será determinado por las declaraciones de prácticas de certificación o el acuerdo de suscriptor definido por la CA que emita los certificados.

4.9.13.2 Suspensión de una CA

Se puede suspender una CA emisora, si existe una orden judicial o por decisión de la DGD, o cuando el ECA acredite que la CA emisora incumple las obligaciones que le impone la Ley N°8454 y su reglamento. Para este caso en particular el reglamento define la suspensión de la CA emisora en el artículo 32, como la imposibilidad para el certificador sancionado de expedir nuevos certificados digitales o de renovar los que expiren durante el plazo de suspensión. Esta suspensión no afectará a los certificados emitidos previamente.

4.9.14 Quién puede solicitar la suspensión

De pleno derecho, el suscriptor del certificado puede solicitar la suspensión de su propio certificado.
Asimismo, pueden solicitar la suspensión otros participantes según el tipo de certificado:

Certificados de CA y certificados de autoridad de sellado de tiempo (TSA)

- El representante legal o apoderado con poderes suficientes de la CA emisora o TSA.
- El Ente Costarricense de Acreditación.
- La autoridad judicial competente.
- La Dirección a cargo de certificadores de firma digital.

Certificados de firma digital y autenticación de persona física

- La autoridad judicial competente.
- La CA emisora.
- La Dirección a cargo de certificadores de firma digital.

Certificados de sello electrónico y agente electrónico de persona jurídica

- El representante legal o representante con facultades suficientes de la persona jurídica suscriptora del certificado, o el tramitador de certificados digitales de persona jurídica vigente y debidamente registrado ante la CA emisora.
- La autoridad judicial competente.
- La CA emisora.
- La Dirección a cargo de certificadores de firma digital.

4.9.15 Procedimiento para la solicitud de suspensión

El procedimiento de suspensión depende del tipo de certificado y del solicitante de la suspensión, de acuerdo con:

Certificados de CA emisora o TSA

- El representante legal o apoderado con poderes suficientes de la CA emisora debe:
    - Presentar un documento de identificación legalmente aceptado y vigente, así como la personería jurídica vigente (con menos de un mes de emitida) donde se establezca su relación como representante legal o apoderado con poderes suficientes de la empresa o institución suscriptora del certificado.
    - Implementar los controles y procedimientos para no expedir nuevos certificados digitales o de renovar los que expiren durante el plazo de suspensión.
- Ente Costarricense de Acreditación (ECA)
    - Comunicar a la DGD el incumplimiento de la acreditación o de las obligaciones que imponen la Ley N°8454, Ley de certificados, firmas digitales y documentos electrónicos y su reglamento.
- La autoridad judicial competente
    - Remitir a la DGD la resolución en la que se ordena la suspensión, los alcances y los plazos de la misma.
- La DGD
    - Notificar a la CA correspondiente las razones por las cuales se le va a suspender.
    - Recibir las pruebas de descargo correspondientes, en caso de que las hubiera.
    - Comunicar a las CA emisoras la resolución correspondiente.

Certificados de firma digital y autenticación de persona física

- Suscriptor del certificado
    - Puede presentarse ante una RA de la CA que emitió el certificado y solicitar la suspensión.
    - Puede solicitar la suspensión vía web, mediante la utilización de un mecanismo de verificación previamente definido para autorizar el proceso de revocación, por ejemplo, comprobación de una frase de desafío, comprobación de preguntas de seguridad, confirmación de correo electrónico, segundo factor de autenticación, entre otras que suministró durante el proceso de aplicación del certificado.
    - Puede solicitar la suspensión a través del centro de atención al cliente de la CA que emitió el certificado.
    - Por cualquier otro medio autorizado por la DGD y que cumpla con un mecanismo de autenticación robusto.
- La autoridad judicial competente
    - Remitir a la DGD la resolución en la que se ordena la suspensión, los alcances y los plazos de la misma.

- La DGD comunica a la CA emisora respectiva, la resolución judicial para suspender el certificado de firma digital emitido para el suscriptor en cuestión.

- La CA emisora
  - Contar con las justificaciones para emitir la suspensión.
  - Si la suspensión es recurrida ante la Dirección de Gobernanza Digital, la CA emisora debe esperar la resolución de la DGD para suspender el certificado.
  - Si fuera el caso, se procede con la suspensión (o revocación) del certificado.

Certificados de sello electrónico y agente electrónico de persona jurídica

- El representante legal o representante con facultades suficientes de la persona jurídica suscriptora del certificado, o el tramitador de certificados digitales de persona jurídica vigente y debidamente registrado ante la CA emisora debe:
  - Presentar ante la autoridad de registro correspondiente, la documentación que lo acredita como representante legal o representante con facultades suficientes o tramitador de certificados digitales de la persona jurídica.
  - Solicitar la suspensión del certificado.
- La autoridad judicial competente:
  - Remitir a la DGD la resolución en la que se ordena la suspensión, los alcances y los plazos de la misma.
- La CA emisora:
  - Contar con las justificaciones para emitir la suspensión.
  - Si la suspensión es recurrida ante la Dirección de Gobernanza Digital, la CA emisora debe esperar la resolución de la DGD para suspender el certificado.
  - Si fuera el caso, se procede con la suspensión (o revocación) del certificado.

4.9.16 Límites del periodo de suspensión

De acuerdo con el artículo 8 del reglamento de la Ley N°8454 de certificados, firmas digitales y documentos electrónicos, la suspensión (o revocación) se mantendrá por todo el plazo en que subsista la causal que le dio origen.

4.10 Servicios de estado de certificado

4.10.1 Características operacionales

El estado de los certificados debe estar disponible a través de los CRL publicados en un sitio Web (en el URL especificado en el CP) y para las CA emisoras de certificados de firma digital de personas físicas, es obligatorio implementar un servicio OCSP.

4.10.2 Disponibilidad del servicio

La CA debe mantener los servicios de verificación del estado de los certificados disponibles 24 x 7 x 365.

4.10.3 Características opcionales

El servicio OCSP, que permite consultar el estado de certificados es una característica opcional para la CA de la Raíz y las CAs de políticas. Sin embargo, para las CA emisoras constituye una característica obligatoria.

4.11 Finalización de la suscripción

Un suscriptor puede finalizar su suscripción de las siguientes formas:

- Revocando su certificado antes del vencimiento (fecha de expiración).
- Cuando expira el certificado.

4.12 Custodia y recuperación de llave

4.12.1 Política y prácticas de custodia y recuperación de llave de cifrado

La CA no debe administrar, custodiar o permitir la recuperación de llaves cuyo propósito sea el de cifrado de información perteneciente a un suscriptor.

4.12.2 Políticas y prácticas de recuperación y encapsulación de llave de sesión

Sin estipulaciones para esta sección.

5. Controles operacionales, de gestión y de instalaciones

La Autoridad Certificadora Raíz mantiene controles de seguridad no-técnicos (esto es, controles físicos, procedimientos y de personal) para asegurar la ejecución de las funciones de generación de llave, autenticación de los sujetos, emisión del certificado, revocación del certificado, auditoría y almacenamiento.

5.1 Controles físicos

5.1.1 Localización y construcción del sitio

Las operaciones de la CA deben estar dentro de un ambiente de protección física que impida y prevenga usos o accesos no autorizados o divulgación de información sensible.
Las instalaciones de la CA deben contar con al menos cuatro perímetros de seguridad física (área de recepción, área de servicios de soporte - climatización, energía, comunicaciones, etc.-, área de operación de la CA, área de custodia de material criptográfico). Un perímetro es una barrera o entrada que provee un control de acceso para individuos y requiere una respuesta positiva para proceder a ingresar a la siguiente área. Cada perímetro sucesivo se encuentra más restringido, con controles de acceso más estrictos.
Las instalaciones donde se crean los certificados de la CA se deben proteger con su propio y único perímetro físico, y las barreras físicas (paredes, barrotes) deben ser sólidas, extendiéndose desde el piso real al cielo raso real. Asimismo, estas barreras deben prevenir las emisiones de radiación electromagnética.

5.1.2 Acceso físico

Los controles de acceso físico deben evitar el acceso no autorizado a las instalaciones de la CA. Adicionalmente, el acceso al recinto donde se encuentran las operaciones de la autoridad certificadora debe utilizar controles con 2 factores de autenticación como mínimo (al menos uno de ellos debe ser biométrico).
Cuando las instalaciones operacionales de la CA estén desocupadas, deben estar cerradas con llave y con las alarmas debidamente activadas.
Los perímetros deben ser auditados y controlados para verificar que solo puede tener acceso el personal autorizado debidamente identificado.
Los derechos de acceso a las instalaciones de la CA deben revisarse y actualizarse regularmente, al menos cada seis meses o cuando se presente movimiento en el personal relacionado con labores de operación de la CA.

Los visitantes o personal de servicio de soporte tercerizado que requiera acceso a las instalaciones operacionales de la CA, deben ser escoltados y registrarse el responsable de autorizar el acceso, la fecha y hora de entrada y salida.

5.1.3 Energía y aire acondicionado

El equipo de la autoridad certificadora debe protegerse contra fallas en el fluido eléctrico corriente y otras anomalías en la energía.
Las instalaciones de la CA deben estar equipadas con sistemas de energía primario y de respaldo para asegurar continuidad del fluido eléctrico.
Las instalaciones deben contar con sistemas de aire acondicionado redundantes. El equipo instalado para climatizar el recinto, debe ser capaz de controlar la humedad relativa del mismo.

5.1.4 Exposiciones al agua

Las instalaciones de la CA deben ser construidas y equipadas, y contar con procedimientos implementados para prevenir inundaciones y otros daños por exposición al agua.

5.1.5 Prevención y protección contra fuego

Las instalaciones de la CA deberán contar con procedimientos implementados para la prevención y protección al fuego. Además de ser construidas y equipadas para prevenir, detectar y suprimir incendios o daños producidos por la exposición a llamas o humo.

5.1.6 Almacenamiento de medios

La CA debe asegurar el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensitivos del sistema, contra daños accidentales (agua, fuego, electromagnetismo) y debe impedir, detectar y prevenir su uso no autorizado, acceso o su divulgación.

5.1.7 Eliminación de residuos

La CA debe implementar controles para la eliminación de residuos (papel, medios, equipos y cualquier otro desecho) con el fin de prevenir el uso no autorizado, el acceso o divulgación de información privada y confidencial contenida en los desechos.

5.1.8 Respaldo fuera de sitio

La CA debe mantener respaldos de los datos críticos del sistema y de cualquier otra información sensitiva, incluyendo los datos de auditoría, en una instalación segura fuera del sitio principal.

5.2 Controles procedimentales

5.2.1 Roles de confianza

Los empleados, contratistas y consultores designados para gestionar la infraestructura de confianza deben ser considerados “personas de confianza” sirviendo en “roles de confianza”.
Los roles de confianza deben incluir, al menos, roles que contemplen las siguientes responsabilidades:

a. responsabilidad general de administrar la implementación de las prácticas de seguridad de la CA;
b. aprobación de la generación, revocación y suspensión de los certificados;
c. instalación, configuración y mantenimiento de los sistemas de la CA;
d. operación diaria de los sistemas de la CA, respaldo y recuperación de sistemas;
e. funciones de auditoría interna para ejecutar la inspección y mantenimiento de las bitácoras del sistema de la CA y de los registros de auditoría;
f. funciones de gestión del ciclo de vida de llaves criptográficas (ejemplo, custodios de componentes de llaves);
g. desarrollo de sistemas de la CA.

5.2.2 Número de personas requeridas por tarea

La CA debe establecer, mantener y ejecutar procedimientos de control rigurosos para asegurar la segregación de funciones, basados en las responsabilidades del trabajo y la cantidad de personas de confianza que ejecutan las tareas sensitivas.

5.2.3 Identificación y autenticación para cada rol

La CA debe confirmar la identidad y autorización de todo el personal que intente iniciar labores de confianza. La autenticación de la identidad debe incluir la presencia física de la persona y una verificación por medio de documentos vigentes de identificación legalmente reconocidos, tales como la cédula de identidad para los ciudadanos costarricenses, o el documento único de permanencia, en caso de extranjeros.

5.2.4 Roles que requieren separación de funciones

Los roles que requieren separación de los deberes incluyen (pero no está limitado) a los encargados de ejecutar las siguientes responsabilidades:

- La validación de información en aplicaciones de certificado y de solicitudes o información del suscriptor.
- La aceptación, rechazo, otros procesamientos de la aplicación de certificado, solicitud de revocación, información de afiliación.
- La emisión, o revocación de los certificados, incluyendo personal con acceso a porciones restringidas del repositorio.
- La generación, emisión o destrucción de los certificados de la CA.
- La puesta en operación de la CA en producción.
- La auditoría interna de la operación de la CA y RA debe ser ejecutada por un rol particular.

5.3 Controles de personal

5.3.1 Requerimientos de experiencia, capacidades y autorización

Las personas seleccionadas para laborar en roles de confianza deben contar con un contrato y deben:

- Haber aprobado exitosamente el programa de entrenamiento apropiado.
- Haber demostrado capacidad para ejecutar sus deberes.
- Haber aceptado las cláusulas de confidencialidad.
- No poseer otros deberes que puedan interferir o causar conflicto con los de la CA.
- No tener antecedentes de negligencia o incumplimiento de labores.
- No tener antecedentes penales.

5.3.2 Procedimientos de verificación de antecedentes

La CA debe contar con procedimientos para verificar la experiencia y los antecedentes del personal que intenta obtener un rol de confianza. Algunos aspectos de la investigación de antecedentes incluyen:

- Confirmación de empleos anteriores.
- Verificación de referencias profesionales.
- Título académico obtenido.

- Solicitud de antecedentes criminales.

La solicitud de antecedentes criminales debe ser repetida para el personal de confianza en operación continua al menos una vez cada tres años.

Los antecedentes deben ser evaluados por la CA para tomar las acciones que sean razonables, de acuerdo al tipo, magnitud y frecuencia del comportamiento descubierto por la investigación respectiva. Los factores revelados en el proceso de verificación pueden ser considerados como motivos para retirar al funcionario del puesto de confianza.

5.3.3 Requerimientos de capacitación

Todo el personal involucrado en las operaciones de la CA debe estar capacitado apropiadamente, en aspectos tales como: operación del software y hardware, políticas y procedimientos organizacionales, procedimientos de seguridad y operativos, y las estipulaciones legales.

5.3.4 Requerimientos y frecuencia de re-capacitación

La CA debe capacitar al personal cuando se presenten cambios significativos en las operaciones de la CA, por ejemplo, cuando se producen actualizaciones de hardware o software, cambios en los sistemas de seguridad, etc.
La CA debe proveer los programas de entrenamiento y actualización a su personal para asegurar que el personal mantiene el nivel requerido de eficiencia para ejecutar sus labores satisfactoriamente.

5.3.5 Frecuencia y secuencia en la rotación de las funciones

La CA debe efectuar una rotación de sus roles de trabajo. La frecuencia de la rotación del personal debe ser al menos: una vez cada cinco años.
Antes de asumir las nuevas labores, el personal debe recibir a una actualización de la capacitación que le permita asumir las tareas satisfactoriamente.

5.3.6 Sanciones para acciones no autorizadas

La CA debe ejecutar las acciones administrativas y disciplinarias apropiadas contra el personal que violente las normas de seguridad establecidas en esta política o su CPS, de acuerdo a lo estipulado en el contrato de trabajo definido para los roles de confianza. Además, debe llevar un registro de la frecuencia y severidad de las acciones, con el fin de determinar la sanción que debe ser aplicada.

5.3.7 Requerimientos para contratistas independientes

La CA puede contratar personal externo o consultores solamente si existe una relación claramente definida con el contratista y bajo las siguientes condiciones:

- existe un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas.
- no se posee personal disponible para llenar los roles de confianza contratados.
- los contratistas o consultores cumplen con los mismos requisitos del punto 5.3.1.
- una vez finalizado el servicio contratado se revocan los derechos de acceso.

5.3.8 Documentación suministrada al personal

La CA debe suministrar suficiente documentación al personal para que ejecute un rol, donde se definen los deberes y procedimientos para el correcto desempeño de su función.

5.4 Procedimientos de bitácora de auditoría

La CA debe mantener controles para proveer una seguridad razonable de que:

- los eventos relacionados con el ambiente de operación de la CA, la gestión de las llaves y los certificados, son registrados exacta y apropiadamente;
- se mantiene la confidencialidad y la integridad de los registros de auditoría vigentes y archivados;
- los registros de auditoría son archivados completa y confidencialmente;
- los registros de auditoría son revisados periódicamente por personal autorizado.

5.4.1 Tipos de eventos registrados

La CA debe registrar los tipos de eventos que se presentan en sus operaciones. La CA debe mantener las bitácoras manuales o automáticas, indicando para cada evento la entidad que lo causa, la fecha y hora del mismo. La CA debe registrar los eventos relacionados con:

- la gestión del ciclo de vida de las llaves de la CA;
- la gestión del ciclo de vida del dispositivo criptográfico;
- la gestión del ciclo de vida del sujeto de certificado;
- la información de solicitud de certificados;
- la gestión del ciclo de vida del certificado;
- los eventos sensibles de seguridad;

Las bitácoras de auditoría no deben registrar las llaves privadas de ninguna forma y los relojes del sistema de cómputo de la CA deben estar sincronizados con el servicio de tiempo UTC-6 para un registro exacto de los eventos.

5.4.2 Frecuencia de procesamiento de la bitácora

El personal de la CA emisora con el rol de auditor debe realizar al menos tres revisiones por año de las bitácoras de auditoría, sin necesidad de ser avisadas; mientras que la CA de la Raíz debe realizar al menos una revisión anual de las bitácoras.
Además de las revisiones oficiales, las bitácoras de auditoría deben ser revisadas en respuesta a una alerta, por irregularidades o incidentes dentro de los sistemas de la CA.
El procesamiento de la bitácora de auditoría consiste en una revisión de las bitácoras y la documentación de los motivos para los eventos significativos, y todas las acciones deben ser documentadas.
Las bitácoras de auditorías actuales y archivadas deben ser recuperadas solamente por personal autorizado, ya sea por razones válidas del negocio o por seguridad.

5.4.3 Periodo de retención para la bitácora de auditoría

Las bitácoras de auditoría deben ser mantenidas en el sistema por al menos dos meses posteriores a su procesamiento y deberán ser archivadas de acuerdo a la sección 5.5.2.

5.4.4 Protección de bitácora de auditoría

Las bitácoras de auditorías actuales o archivadas deben mantenerse de forma que se prevenga su revelación, modificación, destrucción no autorizada o cualquier otra intromisión.

5.4.5 Procedimientos de respaldo de bitácora de auditoría

La CA debe mantener copias de respaldo de todos los registros auditados.

5.4.6 Sistema de recolección de auditoría (interno vs. externo)

Los procesos de auditoría de seguridad deben ejecutarse independientemente y no deben, de ninguna forma, estar bajo el control de la CA, los procesos de auditoría deben ser invocados al iniciar el equipo y terminarlos solo cuando el sistema es apagado.

En caso de que el sistema automatizado de auditoría falle, la operación de la CA debe cesar hasta que las capacidades de auditoría puedan ser reestablecidas.

5.4.7 Notificación al sujeto que causa el evento

Cuando un evento es almacenado por la bitácora, no se requiere notificar al causante de dicho evento.

5.4.8 Evaluación de Vulnerabilidades

La CA y el personal operativo deben estar vigilantes de intentos para violar la integridad del sistema de generación de certificados, incluyendo equipo, localización física y personal. Las bitácoras deben ser revisadas por un auditor de seguridad para los eventos que poseen acciones repetitivas, solicitudes para información privilegiada, intentos de acceso al sistema de archivos y respuestas no autenticadas.
Los equipos donde se ejecutan las operaciones de la CA emisora deben someterse a análisis semestrales de vulnerabilidades.

5.5 Archivado de registros

5.5.1 Tipos de registros archivados

La CA debe almacenar los registros para establecer la validez de una firma y de la operación propia de la infraestructura PKI. Se deben archivar los siguientes datos:

Durante la inicialización del sistema de la CA:

- la acreditación de la CA (si es necesaria);
- el CP y el CPS;
- cualquier acuerdo contractual para establecer los límites de la CA;
- la configuración del sistema.

Durante la operación de la CA:

- modificaciones o actualizaciones de cualquiera de los ítems anteriores;
- solicitudes de certificados o de revocación;
- documentación para autenticar la identidad del suscriptor;
- documentación de recepción y aceptación del certificado;
- documentación de recepción de dispositivos de almacenamiento de llaves;
- todos los certificados y CRLs (información de revocación) tanto emitidos o publicados;
- bitácoras de auditoría;
- otros datos o aplicaciones para verificar el contenido de los archivos;
- todos los trabajos comunicados o relacionados a políticas, otras CA y cumplimiento de auditoría.

5.5.2 Periodos de retención para archivo

Todos los archivos deben mantenerse por un periodo de al menos diez años. Además de mantener los controles para que los archivos puedan ser leídos durante el periodo de retención definido.

5.5.3 Protección de archivo

Los archivos no deben modificarse o eliminarse por alguna operación no autorizada del equipo de la CA. La CA debe mantener la lista de personas autorizadas a mover los registros a otros medios.
Los medios de almacenamientos deben estar guardados en instalaciones seguras, los registros deben ser etiquetados con un nombre distintivo, la fecha y hora de almacenamiento y la clasificación del tipo de información.

5.5.4 Procedimientos de respaldo de archivo

La CA debe mantener procedimientos adecuados de respaldo de archivos (físicos y electrónicos), tanto en el sitio principal como en el alterno, que aseguren la disponibilidad de los mismos, de acuerdo a un análisis de riesgos determinado por los factores de operación de la CA.

5.5.5 Requerimientos para sellado de tiempo de registros

Los certificados, las listas de revocación (CRL) y otras entradas en la base de datos de revocación debe contener información de fecha y hora. Esta información de fecha y hora no necesita tener una base criptográfica, pero si debe estar sincronizada con el servicio de tiempo de la UTC-6.

5.5.6 Sistema de recolección de archivo (interno o externo)

Los sistemas de archivos de la CA son internos al ámbito de sus operaciones y deben conservar las pistas de auditoría.

5.5.7 Procedimientos para obtener y verificar la información archivada

Solamente el personal de confianza autorizado está habilitado para obtener acceso al archivo. La CA debe realizar pruebas de restauración de la información archivada al menos una vez al año. La integridad de la información debe ser verificada cuando es restaurada.

5.6 Cambio de llave

La CA debe cambiar periódicamente sus llaves de firma, de acuerdo con los años de validez de sus certificados en la jerarquía nacional de certificadores registrados (tiempo de uso) y considerando que el último certificado otorgado debe poder ser verificado durante su vigencia (tiempo operacional).

Los responsables de la CA tendrán la obligación de garantizar que el tiempo máximo de uso en años de los certificados de niveles inferiores se ajusta con el tiempo operacional de todos los niveles superiores.

5.7 Recuperación de desastre y compromiso

5.7.1 Procedimientos para el manejo de incidente y compromiso

La CA debe contar con políticas y procedimientos formales para el reporte y atención de incidentes.
Los funcionarios ejecutando roles de confianza deben velar por la seguridad de las instalaciones y la CA debe mantener procedimientos para que estos funcionarios reporten los incidentes.
La CA debe mantener un plan de recuperación de desastres, si el equipo de la CA es dañado entonces las operaciones de la CA deben reestablecerse lo más pronto posible, dando prioridad a la capacidad de revocar certificados de suscriptor.
Si la CA no puede ser reestablecida dentro de una semana, entonces su llave se reporta como comprometida y todos sus certificados son revocados. En casos excepcionales, la DGD puede otorgar extensiones para la CA.

5.7.2 Corrupción de datos, software y/o recursos computacionales

Posterior a una corrupción de recursos computacionales, software o datos, la CA afectada debe realizar, en forma oportuna, un reporte del incidente y una respuesta al evento.

5.7.3 Procedimientos de compromiso de llave privada de la entidad

La CA debe mantener controles para brindar una seguridad razonable de que la continuidad de las operaciones se mantenga en caso de compromiso de las llaves privadas de la CA. Para los efectos de Plan de Continuidad de Negocio, las llaves privadas de las CA deben estar en custodia y respaldadas bajo estrictas normas de seguridad, y almacenadas en dispositivos criptográficos FIPS 140-2 nivel 3, que garantizan la no divulgación de las llaves.
Los planes de continuidad del negocio de la CA deben referirse al compromiso o sospecha de compromiso de las llaves privadas de la CA como un desastre.
En caso de que la llave de la CA se haya comprometido, el superior de la CA deberá revocar el certificado de CA, y la información de la revocación debe publicarse inmediatamente.

5.7.4 Capacidad de continuidad del negocio después de un desastre

La CA debe contar con un proceso administrativo para desarrollar, probar, implementar y mantener sus planes de continuidad del negocio.
La CA debe desarrollar, probar, mantener e implementar un plan de recuperación de desastres destinado a mitigar los efectos de cualquier desastre natural o producido por el hombre. Los planes de recuperación de desastres se enfocan en la restauración de los servicios de sistemas de información y de las funciones esenciales del negocio.
El sitio alterno debe contar con protecciones de seguridad física equivalentes al sitio principal.
El sitio alterno, deben tener la capacidad de restaurar o recobrar operaciones esenciales dentro de las veinticuatro horas siguientes al desastre, con al menos soporte para las siguientes funciones: revocación de certificados y publicación de información de revocación.

5.8 Terminación de una CA o RA

En caso de que la terminación de la CA se dé por conveniencia, reorganización, o por otras razones que no estén relacionadas con la seguridad, entonces se deben tomar las previsiones antes de terminar la CA para evitar el compromiso de toda la infraestructura. En este caso, puede ser que ningún certificado firmado por la CA deba ser revocado.
En caso de que la terminación de la CA esté relacionada con eventos de seguridad, entonces la CA debe considerarse como una CA comprometida.
Antes de la terminación de la CA, toda la información relacionada con la operación de la CA debe ser enviada a la DGD para su custodia.
Cuando se presenta la terminación de una RA, todos los archivos de datos deben ser enviados a la CA respectiva para su custodia.
Si se presenta un compromiso de la llave de la CA o un desastre donde las instalaciones de la CA están físicamente dañadas y todas las copias de las llaves de firma de la CA están destruidos, entonces la CA debe solicitar que se revoque su certificado.
Cada CA o RA debe desarrollar un plan de terminación que minimice el impacto y la interrupción del servicio provisto a los clientes, suscriptores y partes que confían. Dicho plan debe darle tratamiento al menos a los siguientes puntos:

- Notificación a las partes afectadas asumiendo el costo de la misma.
- Procedimiento de revocación del certificado (de la CA, CA subordinadas, los utilizados en RA para sus operaciones, suscriptores, etc. según sea el caso).
- La preservación de toda la información en concordancia con este CP y la normativa aplicable.
- La continuación de los servicios de validación de los certificados y de soporte a los suscriptores.

- Procedimientos para la eliminación de las llaves privadas y del hardware que las contiene.
- Disposiciones para la transición de los servicios a una CA sucesora.

6. Controles técnicos de seguridad

En esta sección se definen las medidas de seguridad tomadas por la CA para proteger sus llaves criptográficas y los datos de activación. La gestión de las llaves es un factor crítico que permite asegurar que todas las llaves privadas están protegidas y solamente pueden ser activadas por personal autorizado.

6.1 Generación e instalación del par de llaves

La CA mantendrá controles para brindar seguridad razonable de que los pares de llaves de la CA, se generan e instalan de acuerdo con el protocolo definido para la generación de llaves.

6.1.1 Generación del par de llaves

El proceso de generación de llaves ejecutado por la CA previene la pérdida, divulgación, modificación o acceso no autorizado a las llaves privadas que son generadas. Este requerimiento aplica para toda la jerarquía nacional de certificadores registrados hasta llegar a los suscriptores.

Certificados de CA emisora
La CA debe generar las llaves mediante un proceso seguro por medio del módulo criptográfico de hardware, que cumple como mínimo el estándar FIPS 140-2 nivel 3 y a un procedimiento acorde con la "ceremonia de generación de llaves" definida en los lineamientos técnicos. La CA garantiza que la llave privada de firma nunca permanecerá fuera del módulo donde fue generada, a menos que se almacene en un mecanismo de recuperación de llaves.

El proceso de generación de llaves de CA debe producir llaves que:

a. sean apropiadas para la aplicación o propósito destinado y que sean proporcionales a los riesgos identificados;
b. usen un algoritmo aprobado en esta CP, de acuerdo a la sección 7.1.3;
c. tengan una longitud de llave que sea apropiada para el algoritmo y para el período de validez del certificado de la CA, de acuerdo con la sección 6.1.5 de tamaños de llave;
d. tomen en cuenta los requisitos del tamaño de llave de la CA padre (la CA que le emitió el certificado) y subordinada (la CA que recibe el certificado);

Certificados de firma digital y autenticación de persona física en modalidad local
La generación de las llaves de los suscriptores requiere que los módulos de criptografía asociados cumplan al menos con el estándar FIPS 140-2 nivel 2, o bien que posean al menos la certificación Common Criteria EAL 4+ en el perfil de protección SSCD tipo 3.

Certificados de firma digital y autenticación de persona física en modalidad remota
La generación de las llaves privadas de suscriptor debe garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de firma, y que además cuenta con la utilización de un dispositivo criptográfico seguro que cumple con los requisitos de firma digital certificada.
Para esto se debe demostrar en el módulo de activación de firma el cumplimiento de los estándares:

- "Sistemas confiables que permiten firma de servidor. Parte 1: Requisitos generales de seguridad del sistema" (Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements, EN 419 241-1) y

- "Sistemas confiables que permiten firma de servidor. Parte 2: Perfil de protección de QSCD para la firma del servidor" (Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing, EN 419 241-2).

Lo anterior, de conformidad con la valoración positiva del Sistema Nacional de Certificación Digital, de acuerdo con lo establecido en la Ley N°8454 y su reglamento.

Para el proceso de activación o autorización del uso de la llave privada de firma cuando esta se encuentra gestionada de forma remota, se debe usar un módulo criptográfico mantenido bajo el control exclusivo del suscriptor que al menos cuente con protección por software equivalente al estándar FIPS 140-2 nivel 1 o superior, por ejemplo, Trusted Execution Environment (TEE) o bien un elemento seguro por hardware como Secure Element (SE). Las llaves de autorización o activación pueden estar asociadas a un certificado de autenticación de persona física.

Certificados de sello electrónico y agente electrónico de persona jurídica
La generación y el almacenamiento de las llaves de los certificados de persona jurídica no requieren de módulos criptográficos asociados. No obstante, se recomienda a las instituciones que los desean utilizar que los módulos de criptografía cumplan al menos con el estándar FIPS 140-2 nivel 3, o bien que posean al menos la certificación Common Criteria EAL 4+ en el perfil de protección SSCD tipo 3.

Certificados de autoridad de sellado de tiempo (TSA)
La TSA debe generar las llaves mediante un proceso seguro, con un módulo criptográfico de hardware, que cumpla al menos con el estándar FIPS 140-2 nivel 3.

6.1.2 Entrega de la llave privada al suscriptor

Se debe generar y mantener la llave privada dentro de los límites del módulo criptográfico, es decir el módulo criptográfico debe generar la llave privada localmente.

6.1.3 Entrega de la llave pública al emisor del certificado

Las llaves públicas transferidas deben ser entregadas a través de mecanismos que aseguren que la llave pública no se altera durante el tránsito.

Certificados de CA emisora
La llave pública debe ser entregada mediante un método fuera de banda, tal como:

- almacenado en un módulo criptográfico de la entidad;
- otros medios seguros que garanticen autenticidad e integridad.

Certificados de firma digital y autenticación de persona física
La llave pública debe ser entregada por la RA a través de medios legibles por computadoras desde una fuente autenticada;

Certificados de sello electrónico y agente electrónico de persona jurídica
La llave pública debe ser distribuida utilizando uno o varios de los siguientes métodos:

- medios legibles por computadoras desde una fuente autenticada;
- almacenado en un módulo criptográfico de la entidad;
- otros medios seguros que garanticen autenticidad e integridad.

Certificados de autoridad de sellado de tiempo (TSA)
La llave pública debe ser entregada mediante un método fuera de banda, tal como:

- almacenado en un módulo criptográfico de la entidad;

- otros medios seguros que garanticen autenticidad e integridad.

6.1.4 Entrega de la llave pública de la CA a las partes que confían

La distribución de la llave pública se realiza a través del certificado digital y del repositorio público respectivo.

6.1.5 Tamaños de llave

El tamaño de las llaves debe ser suficientemente largo para prevenir que otros puedan determinar la llave privada utilizando cripto-análisis durante el periodo de uso del par de llaves.

Certificados de CA emisora
Las llaves de la CA deben tener un tamaño de acuerdo con los lineamientos de la industria y las mejores prácticas. Para la CA raíz y las CA de Políticas debe tener como mínimo de 4096 bits para el algoritmo RSA o 384 bits mínimo para el algoritmo ECC. Para las CA emisoras debe tener un tamaño mínimo de 2048 bits para el algoritmo RSA o 384 bits mínimo para el algoritmo ECC.

Certificados de firma digital y autenticación de persona física y certificados de sello electrónico y de agente electrónico de persona jurídica y de TSA
El tamaño de las llaves para el suscriptor como mínimo deben tener un largo de 2048 bits para el algoritmo RSA o 384 bits mínima para el algoritmo ECC. La longitud de la llave pública que será certificada por la CA, debe ser menor o igual al tamaño de la llave privada de firma de la CA.

6.1.6 Generación de parámetros de llave pública y verificación de calidad

La CA genera y verifica los parámetros de llave pública de acuerdo con el estándar FIPS 186-2 (Digital Signature Standard-DSS) que define el cripto-algoritmo utilizado en la generación.

6.1.7 Propósitos de uso de llave (Campo “keyusage” de X.509 v3)

Certificados de CA emisora
La CA Raíz únicamente podrá emitir certificados de firma para las Autoridades de Políticas y para las CRL respectivas. Las CAs de políticas únicamente podrán emitir certificados de firma a las CA emisoras y para sus CRLs.
La CA emisora no puede emitir certificados con el uso de encripción.

Certificados de firma digital y autenticación de persona física
Los suscriptores tendrán dos certificados emitidos uno con el uso de firma digital y el otro con el uso de autenticación.

- Para firmar: digitalSignature + nonRepudiation
- Para autenticarse: digitalSignature + keyEncipherment

Certificados de sello electrónico y agente electrónico de persona jurídica
Los suscriptores tendrán dos certificados emitidos uno con el uso de sello electrónico (firma digital) y el otro con el uso de agente electrónico (autenticación).

- Para sello electrónico: digitalSignature + nonRepudiation
- Para agente electrónico: digitalSignature + keyEncipherment + dataEncipherment

6.2 Controles de ingeniería del módulo criptográfico y protección de la llave privada

6.2.1 Estándares y controles del módulo criptográfico

Certificados de CA emisora

La CA debe mantener controles para asegurar que las llaves privadas de la CA permanecen confidenciales y mantienen su integridad y el acceso al hardware criptográfico de la CA está limitado a individuos autorizados.
Las llaves privadas de la CA deben ser respaldadas, guardadas y recuperadas por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro.
Las copias de respaldo de las llaves privadas de la CA Raíz deben estar sujetas al mismo o mayor nivel de controles de seguridad que las llaves que actualmente están en uso. La recuperación de las llaves de la CA debe llevarse a cabo de una forma tan segura como el proceso de respaldo.
El estándar de módulos criptográficos es el "Security Requirements for Cryptographics Modules" (actualmente FIPS140). Los módulos criptográficos para las CAs Emisoras deben certificarse como mínimo con el FIPS 140-2 nivel 3.

Certificados de firma digital y autenticación de persona física en modalidad local
El suscriptor debe cumplir con los controles definidos en el acuerdo de suscriptor y utilizar módulos criptográficos basados como mínimo en el estándar FIPS 140-2 nivel 2, o bien que posean al menos la certificación Common Criteria EAL 4+ en el perfil de protección SSCD tipo 3.

Certificados de firma digital y autenticación de persona física en modalidad remota
La CA debe mantener los controles que garanticen que las llaves custodiadas de firma del suscriptor permanecen confidenciales y mantienen su integridad, por lo que el acceso al hardware criptográfico está limitado únicamente a individuos autorizados.
Las llaves privadas custodiadas deben ser respaldadas, guardadas y recuperadas por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro.
Debe existir un procedimiento desarrollado por la CA que garantice la seguridad de la recuperación de las llaves que custodia y su respectivo respaldo.
Los módulos criptográficos deben certificarse como mínimo con el estándar FIPS 140-2 nivel 3 o bien que cumplan al menos la certificación Common Criteria EAL 4+ acorde a la parte 5 del perfil de protección eIDAS EN 419 221-5:2018 para los módulos criptográficos de proveedores de servicios de confianza.

Certificados de sello electrónico y agente electrónico de persona jurídica
Los suscriptores de certificados de persona jurídica deben cumplir con los controles definidos en el acuerdo de suscriptor. En caso de así desearlo, pueden utilizar un módulo criptográfico basado como mínimo en el estándar FIPS 140-2 nivel 3, o bien que posean al menos la certificación Common Criteria EAL 4+ en el perfil de protección SSCD tipo 3.

Certificados de autoridad de sellado de tiempo (TSA)
El certificado de TSA debe cumplir con los controles definidos en el acuerdo de suscriptor y utilizar un módulo criptográfico basado como mínimo en el estándar FIPS 140-2 nivel 3.

6.2.2 Control multi-persona de llave privada (m de n)

Certificados de CA emisora
Para la activación de la llave privada de firma de la CA se debe utilizar controles de acceso de múltiples partes (es decir, "m" de "n") con un valor mínimo de 3 para "m".
Si las llaves privadas de la CA son respaldadas, estas deben ser respaldadas, guardadas y recuperadas por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro. La cantidad de personal autorizado para llevar a cabo esta función debe mantenerse al mínimo.

Certificados de firma digital y autenticación de persona física
Sin estipulaciones.

Certificados de sello electrónico y agente electrónico de persona jurídica

Para la activación de la llave privada de sello electrónico y/o agente electrónico de persona jurídica, se recomienda utilizar controles de acceso que resguarden adecuadamente la llave privada. En caso de disponer de un dispositivo criptográfico para la gestión de la llave privada, una vez que este haya sido activado, se debe mantener resguardado físicamente y monitoreado, para evitar un uso inapropiado.

Certificados de autoridad de sellado de tiempo (TSA)
Para la activación de la llave privada de firma del TSA se debe utilizar controles de acceso de múltiples partes (es decir, "m" de "n") con un valor mínimo de 3 para "m". Una vez activado el dispositivo criptográfico se debe mantener resguardado físicamente y monitoreado, para evitar otros usos.

6.2.3 Custodia de llave privada

La CA no debe implementar servicios de custodia de llaves cuyo propósito sea la recuperación de información que el suscriptor haya cifrado.
La CA podrá custodiar llaves privadas de suscriptores cuando se implemente un modelo de gestión de firma remota, siempre en cumplimiento de los requisitos aplicables a dicho modelo de conformidad con la Ley N°8454, su reglamento y sus políticas.

6.2.4 Respaldo de llave privada

Los respaldos de llaves privadas de la CA son únicamente para propósitos de recuperación en caso de una contingencia o desastre. Los planes de continuidad del negocio de la CA deben incluir procesos de recuperación de desastres para todos los componentes críticos del sistema de la CA, incluyendo el hardware, software y llaves, en el caso de falla de uno o más de estos componentes.
Las copias de respaldo de las llaves privadas de la CA deberían estar sujetas al mismo o mayor nivel de controles de seguridad que las llaves que actualmente están en uso. Debe existir un procedimiento desarrollado por la CA que garantice la seguridad de la recuperación de sus llaves privadas y su respectivo respaldo.

Certificados de firma digital y autenticación de persona física en modalidad local
Las llaves privadas de certificados de firma digital de los suscriptores no son respaldadas por ningún motivo en la CA, y estas permanecen dentro de los límites de los dispositivos criptográficos donde fueron generadas.

Certificados de firma digital y autenticación de persona física en modalidad remota
La CA puede mantener duplicados de los datos de creación de firma únicamente con fines de respaldo, siempre que se cumplan los siguientes requisitos:

- La seguridad de los datos respaldados debe tener el mismo nivel que los datos originales.
- La cantidad de respaldos necesarios para garantizar la continuidad del servicio se debe definir de acuerdo con las buenas prácticas internacionales (indicando cual) y que esta cantidad no comprometa la seguridad de los certificados de firma digital y autenticación de persona física en modalidad remota, por un exceso de respaldos.

6.2.5 Archivado de llave privada

La CA no archiva la llave privada de ninguno de los suscriptores. En el caso de la CA, ésta debe archivar su par de llaves (pública y privada) en forma encriptada en concordancia con las disposiciones de protección de llaves definidas en este CP, por un plazo acorde con la legislación aplicable.

6.2.6 Transferencia de llave privada hacia o desde un módulo criptográfico

Las llaves privadas de la CA son generadas por un módulo criptográfico seguro. En el evento que una llave privada es transportada desde un módulo criptográfico a otro, la llave privada debe estar encriptada durante su transporte.
La llave privada usada para encriptar el transporte de la llave privada debe estar protegida contra divulgación no autorizada.

6.2.7 Almacenamiento de la llave privada en el módulo criptográfico

Los dispositivos criptográficos utilizados para el almacenamiento del respaldo de las llaves privadas de la CA deben ser guardados de forma segura, en un sitio alterno, para que sean recuperados en el caso de un desastre en el sitio primario
Las partes de la clave secreta o los componentes necesarios para usar y gestionar los dispositivos criptográficos de recuperación de desastres, deberían estar también guardados con seguridad en una ubicación fuera del sitio primario.
Las llaves privadas de la CA deben ser almacenadas y utilizadas dentro de un dispositivo criptográfico seguro que cumpla como mínimo con el perfil de protección apropiado de los requisitos del estándar FIPS 140-2 nivel 3

6.2.8 Método de activación de llave privada

Certificados de CA emisora
Los métodos de activación de llaves de la CA están protegidos y para accederlos se 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.

Certificados de firma digital y autenticación de persona física
Los métodos de activación de llaves para un usuario deben contar con al menos un factor de seguridad.

Certificados de firma digital y autenticación de persona física en modalidad local
Los métodos de activación de llaves para un usuario deben contar con al menos un factor de seguridad.

Certificados de firma digital y autenticación de persona física en modalidad remota
La activación de las llaves privadas custodiadas de forma remota debe realizarse únicamente por un suscriptor autenticado, se debe garantizar que no sean reveladas a ningún tercero que no sea el propietario de las llaves, por lo que se requiere el uso de al menos dos factores de autenticación segura.

Certificados de sello electrónico y agente electrónico de persona jurídica
Los métodos de activación de llaves para un usuario deben contar con al menos un factor de seguridad.

Certificados de autoridad de sellado de tiempo (TSA)
Los métodos de activación de llaves de autoridades de sellado de tiempo están protegidos mediante una combinación de al menos dos factores de seguridad. Los datos de activación deben estar distribuidos en roles de confianza que ejecutan diversas personas.

6.2.9 Método de desactivación de llave privada

Certificados de CA emisora
Para la CA Raíz y de Políticas es obligatorio que los módulos criptográficos, los cuales han sido activados, no estén desatendidos o abiertos al acceso no autorizado. Después de usarlos, estos deben ser desactivados manualmente o por un tiempo de expiración por estado pasivo. Los módulos de hardware criptográfico deben ser removidos y almacenados cuando no estén en uso.

En el caso de las CA emisoras los equipos se mantienen en línea, para dichos efectos una vez activados los dispositivos criptográficos, estos se deben mantener monitoreados y protegidos contra accesos no autorizados.

Certificados de firma digital y autenticación de persona física
Sin estipulaciones.

Certificados de sello electrónico y agente electrónico de persona jurídica
Cuando los equipos que hospedan los certificados de persona jurídica se encuentran en línea, estos se deben mantener monitoreados y protegidos contra accesos no autorizados.

Certificados de autoridad de sellado de tiempo (TSA)
Cuando los equipos que hospedan el certificado sellado de tiempo se encuentran en línea, estos se deben mantener monitoreados y protegidos contra accesos no autorizados. Cuando los equipos no estén en uso entonces los módulos de hardware criptográfico deben ser removidos y almacenados.

6.2.10 Método de destrucción de llave privada

El procedimiento para la destrucción de llaves privadas debe incluir la autorización para destruirla.

Certificados de CA emisora
La CA raíz, las CA de políticas y la CA emisora deben destruir los respaldos de las llaves privadas que han expirado. Para los módulos criptográficos de hardware, estos deben ser limpiados por medio de inicialización de ceros (Zeroize Command).

Certificados de firma digital y autenticación de persona física en modalidad local
Los módulos criptográficos de hardware que hospedan la llave privada deben ser limpiados por medio de inicialización de ceros (Zeroize Command).

Certificados de firma digital y autenticación de persona física en modalidad remota
Las llaves privadas deben destruirse cuando ya no sean necesarias, o cuando los Certificados Digitales a los que correspondan expiren o sean revocados, eliminándolas de cualquier repositorio criptográfico y medios de exportación o respaldo, si aplica, todo lo anterior deberá hacerse constar por medio de una comunicación oficial al suscriptor.

Certificados de sello electrónico y agente electrónico de persona jurídica
Cuando sean utilizados, los módulos criptográficos de hardware que hospedan la llave privada deben ser limpiados por medio de inicialización de ceros (Zeroize Command).

Certificados de autoridad de sellado de tiempo (TSA)
La TSA debe destruir los respaldos de las llaves privadas que han expirado. Para los módulos criptográficos de hardware, estos deben ser limpiados por medio de inicialización de ceros (Zeroize Command).

6.2.11 Clasificación del módulo criptográfico

Certificados de CA emisora
La capacidad del módulo criptográfico de la CA emisora es expresada en cumplimiento como mínimo del estándar FIPS 140-2, nivel 3.

Certificados de firma digital y autenticación de persona física en modalidad local
El módulo criptográfico para los suscriptores de certificados de firma digital y autenticación debe cumplir como mínimo con el estándar FIPS 140-2, nivel 2, o bien debe poseer al menos la certificación Common Criteria EAL 4+ en el perfil de protección SSCD tipo 3.

Certificados de firma digital y autenticación de persona física en modalidad remota
El módulo criptográfico para la generación y almacenamiento de las llaves privadas de suscriptor deben cumplir como mínimo con el estándar FIPS 140-2 nivel 3 o superior, o bien posea al menos la certificación Common Criteria EAL 4+ acorde a la parte 5 del perfil de protección eIDAS EN 419 221-5:2018 para los módulos criptográficos de proveedores de servicios de confianza.

Certificados de sello electrónico y agente electrónico de persona jurídica
No es requerido un módulo criptográfico para la gestión de las llaves privadas de los certificados digitales de persona jurídica. No obstante, se les sugiere a las instituciones que así lo deseen, contar con un módulo criptográfico para los certificados de persona jurídica que cumpla como mínimo con el estándar FIPS 140-2, nivel 3, o bien que estos posean al menos la certificación Common Criteria EAL 4+ en el perfil de protección SSCD tipo 3.

Certificados de autoridad de sellado de tiempo (TSA)
El almacenamiento de las llaves privadas de la TSA debe cumplir como mínimo con el estándar FIPS 140-2, nivel 3

6.3 Otros aspectos de gestión del par de llaves

Las CA de la jerarquía nacional de certificadores registrados deben establecer los medios necesarios para gestionar en forma segura las llaves de los suscriptores durante el ciclo de vida de las mismas.

6.3.1 Archivado de la llave pública

La CA debe mantener controles para sus propias llaves, de acuerdo a lo estipulado en la sección 5.5. Las llaves archivadas de la CA deberían estar sujetas al mismo o mayor nivel de control de seguridad que las llaves que están en uso actualmente.

6.3.2 Periodo operacional del certificado y periodo de uso del par de llaves

Los períodos de uso de las llaves públicas y las llaves privadas coincidirán con el período de uso del certificado digital que vincula la llave pública.
Los periodos máximos de validez y uso de los certificados y las llaves emitidas según esta CP son descritos en la siguiente tabla:

Nivel de jerarquía	Tiempo de uso máximo en años	Tiempo operacional máximo en años	Descripción
Certificados de firma digital de persona física	4	4	El par de llaves utilizado para la emisión de estos certificados se crean con cada emisión, y por tanto tienen una validez máxima de hasta cuatro (4) años.
Certificados de autenticación de persona física	4	4	El par de llaves utilizado para la emisión de estos certificados se crean con cada emisión, y por tanto tienen una validez máxima de hasta cuatro (4) años.
Certificados de sello electrónico de persona jurídica	4	4	El par de llaves utilizado para la emisión de estos certificados se crean con cada emisión, y por tanto tienen una validez máxima de hasta cuatro (4) años.
Certificados de agente electrónico de persona jurídica	4	4	El par de llaves utilizado para la emisión de estos certificados se crean con cada emisión, y por tanto tienen una validez máxima de hasta cuatro (4) años.

CA emisoras	8	12	A la CA emisora se le otorga un certificado con una validez de máximo 8 años, durante ese periodo puede emitir certificados a los usuarios o suscriptores. Sin embargo, el último certificado emitido, antes de vencer su validez, debe tener la misma efectividad, es decir, cuatro años para el usuario o suscriptor. Entonces su tiempo de uso es 8 años (con capacidad para emitir certificados de suscriptor), pero dura cuatro años más en operación para validar las listas de revocación, de ahí que el tiempo operacional es por 12 años.
CA Políticas	12	24	La CA de políticas tiene una validez de máximo 12 años, y el último certificado otorgado a una CA emisora debe garantizar la operación por doce años más. Por estos motivos el periodo operacional de la CA de Políticas debe ser de al menos 24 años.
CA Raíz	24	48	Siguiendo el mismo criterio la validez máxima de la CA Raíz es 24 años, más 24 años que pueda operar la CA de Política, da como resultado los 48 años de tiempo operacional para el certificado de la CA Raíz.

6.4 Datos de activación

La CA mantiene estrictos controles en los datos de activación para operar los módulos criptográficos y que necesitan ser protegidos (ejemplo un PIN, una frase de paso o “password”, una medida biométrica o una parte de llave mantenida manualmente).

6.4.1 Generación e instalación de los datos de activación

Certificados de CA emisora
Se debe contar con datos de activación de múltiples factores para protección de los accesos al uso de llaves privadas y su activación requiere de un control de múltiples partes (es decir, “m” de “n”) con un valor mínimo de tres para “m”.

Certificados de firma digital y autenticación de persona física
Se deben generar e instalar sus propios datos de activación para proteger y prevenir perdidas, robos, modificación, divulgación o uso no autorizado de sus llaves privadas.

Certificados de sello electrónico y agente electrónico de persona jurídica
Se debe contar con controles para protección de los accesos al uso de llaves privadas. En caso de que la institución cuente con un dispositivo criptográfico para la gestión de las llaves de sus certificados de persona jurídica, se requiere generar sus propios datos de activación para prevenir uso no autorizado de la llave privada.

Certificados de autoridad de sellado de tiempo (TSA)
Se debe generar e instalar sus propios datos de activación para proteger y prevenir perdidas, robos, modificación, divulgación o uso no autorizado de sus llaves privadas. Adicionalmente, como parte de los datos de activación se requiere de un control de múltiples partes (es decir, “m” de “n”) con un valor mínimo de tres para “m”.

6.4.2 Protección de los datos de activación

Los datos de activación deberían ser memorizados, sin mantener respaldo escrito. Si se escriben, estos deberían de estar almacenados en un nivel de seguridad semejante al de los módulos criptográficos para protegerlos, y en una localización diferente a la de los módulos criptográficos.

6.4.3 Otros aspectos de los datos de activación

Los datos de activación de los módulos criptográficos de la CA Raíz y CA de Políticas deben ser cambiados al menos una vez cada año. Y en el caso de las CA emisoras o TSA la frecuencia debe ser al menos una vez cada dos meses.

6.5 Controles de seguridad del computador

El equipo de la CA debe usar sistemas operativos que:

- Requieran autenticación para poder ser accedidos
- Provean capacidad para mantener bitácoras y registros de seguridad con fines de auditoría
- Cumplan con requerimientos y controles de seguridad, al menos tan estrictos como los definidos en este CP.

Luego de que la plataforma donde opera el equipo de la CA ha sido aprobada, debe continuar operando bajo los mismos parámetros aprobados.

6.5.1 Requerimientos técnicos de seguridad de computador específicos

Los equipos donde operan los sistemas de la CA, que requieran acceso remoto deben poseer autenticación mutua y los sistemas operativos deberían estar configurados de acuerdo con los estándares del sistema operativo de la CA y ser revisados periódicamente.
Las actualizaciones y parches de los sistemas operativos deberían ser aplicados de manera oportuna y la utilización de programas utilitarios del sistema debería ser restringida al personal autorizado, y debe estar estrictamente controlado.

6.5.2 Clasificación de la seguridad del computador

Los sistemas sensibles de la CA requieren un ambiente informático dedicado y aislado, que implemente el concepto de sede computacional confiable con procesos de auditoría que ejecuten pruebas de seguridad al menos dos veces al año.

6.6 Controles técnicos del ciclo de vida

La CA debe mantener controles en los equipos de seguridad (hardware y software) requeridos para operar en una infraestructura PKI desde el momento de la compra hasta su instalación, de forma que reduzcan la probabilidad que cualquiera de sus componentes sea violentado.
Todo el hardware y software que ha sido identificado para operar las CA debe ser enviado y entregado con métodos que provean una adecuada cadena de custodia.

6.6.1 Controles para el desarrollo de sistemas

La CA debe mantener controles que proporcionen una seguridad razonable de las actividades de desarrollo y mantenimiento de los sistemas de la CA.
Los nuevos sistemas o para la expansión de los sistemas existentes, deben especificar los requisitos de control, seguir procedimientos de prueba de software y control de cambios para la implementación de software.
La CA debe mantener controles sobre el acceso a las bibliotecas fuente de programas.

6.6.2 Controles de gestión de seguridad

Los Administradores de la CA son los responsables de garantizar que se cumplan los procedimientos de seguridad correctamente. Además de ejecutar revisiones periódicas para asegurar el cumplimiento de los estándares de implementación de seguridad.

6.6.3 Controles de seguridad del ciclo de vida

La CA debe incluir controles en la gestión de seguridad por medio de herramientas y procedimientos que verifiquen la adherencia a la configuración de seguridad de los sistemas operativos y redes.

6.7 Controles de seguridad de red

El equipo de la CA debe estar dentro de los límites de la red interna, operando bajo un nivel de seguridad de red crítico. La red de la CA debe estar protegida contra ataques. Los puertos y servicios que no se requieran deben estar apagados.
En el caso de la CA Raíz debe estar off-line y aislada de la red organizacional.
Los niveles críticos de seguridad de red deben incluir:

- El cifrado de las conexiones involucradas con las operaciones de la CA.
- Los sitios Web están provistos de certificados SSL.
- La red está protegida por firewalls y sistemas de detección de intrusos.
- Los accesos externos a información de bases de datos de la CA están prohibidos.
- La CA debe controlar la ruta de acceso del usuario desde la Terminal hasta los servicios.
- Los componentes de la red local deben mantenerse en un ambiente físicamente seguro y sus configuraciones deben ser auditadas periódicamente.
- Los datos sensibles deben encriptarse cuando se intercambian sobre redes públicas o no confiables.

La CA debe definir los procedimientos de control del cambio para el hardware, los componentes de la red y los cambios de configuración del sistema.

6.8 Sellado de tiempo (“Time-Stamping”)

Los certificados, CRL y otras entradas en la base de datos de revocaciones deben contener la fecha y hora, sincronizadas utilizando los servicios UTC-6. El sellado de tiempo es una característica opcional.

7. Perfiles de Certificados, CRL y OCSP

Este capítulo especifica el formato de las CRL y OCSP, tales como información del perfil, versión y extensiones utilizadas. En el caso de la jerarquía nacional de certificadores registrados, los OCSP son un mecanismo opcional para la CA Raíz y las CA de Políticas, debido a que son pocos los certificados emitidos y por tanto revocados por ellas. La verificación del estado de los certificados para las CA emisoras constituye un factor crítico de seguridad para diversas aplicaciones, por lo tanto deben obligatoriamente implementar los dos métodos de validación: OCSP y CRL.

7.1 Perfil del Certificado

Los certificados digitales deben cumplir con:

- Estándar X.509 versión 3.
- RFC3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

- RFC 3039 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- ISO 3166-1 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países”.

Cómo mínimo el certificado contiene:

Campo	Valor o restricciones
Versión	V3, los certificados deben ser X.509 versión 3.
Número de serie	Valor único emitido dentro del ámbito de cada CA emisora.
Algoritmo de firma	El Algoritmo de firma debe ser como mínimo SHA256RSA o como mínimo sha256ECDSA.
Emisor	Nombre de la CA Emisora. Ver sección 7.1.4.
Válido desde	Este campo especifica la fecha y hora a partir de la cual el certificado es válido. Las fechas establecidas para el periodo de validez deben ser sincronizadas con respecto al servicio de tiempo UTC-6.
Válido hasta	Este campo especifica la fecha y hora a partir de la cual el certificado deja de ser válido. Las fechas para la validez del certificado deben ser sincronizadas con el servicio de tiempo UTC-6.
Sujeto	Nombre del suscriptor. Ver sección 7.1.4.
Llave pública del sujeto	Codificado de acuerdo con el RFC 3280. Con un largo de llave mínima de 2048 bits para el algoritmo RSA o 384 bits mínima para el algoritmo ECC.
Identificador de llave de la autoridad	Este campo es usado por los diversos softwares de validación para ayudar a identificar a la autoridad certificadora registrada que emitió el certificado en la cadena de confianza. Referencia el campo “Subject Key Identifier” de la CA emisora del certificado.
Identificador de la llave del sujeto	Este campo es usado por software de validación para ayudar a identificar un certificado que contiene una determinada llave pública.
Política del certificado	Describe las políticas aplicables al certificado, especifica el OID y la dirección URL donde se encuentra disponible el CP respectivo.
Uso de la llave	Debe indicar los usos permitidos de la llave. Este campo debe ser marcado como un CAMPO CRÍTICO. Ver sección 1.4.1 Usos apropiados del certificado
Punto de distribución del CRL	Este campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. En el caso del certificado de la CA Raíz, este atributo no debe especificarse.
Acceso a la información de la autoridad	Este campo es usado para indicar las direcciones donde puede ser encontrado el certificado de la CA emisora. Además, para indicar la dirección donde puede accederse el servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. En el caso del certificado de la CA Raíz, este atributo no debe especificarse.
Usos extendidos de la llave	Referencia otros propósitos de la llave, adicionales al uso. De acuerdo con la sección 7.1.2.5.

Campo	Valor o restricciones
Restricciones básicas	Para el caso de la CA emisora la extensión PathLenConstraint debe ser igual a cero. Ver sección 7.1.2.4 Restricciones básicas.

7.1.1 Número(s) de versión

Todos los certificados emitidos dentro de la jerarquía nacional de certificadores registrados deben ser X.509 versión 3 o superior.

7.1.2 Extensiones del certificado

7.1.2.1 Key Usage

El "key usage" es una extensión crítica que indica el uso del certificado de acuerdo con el RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Ver sección 1.4.1 Usos apropiados del certificado.

7.1.2.2 Extensión de política de certificados

La extensión de "certificatepolicies" del X.509 versión 3 es el identificador del objeto de este CP de acuerdo con la sección 7.1.6. La extensión no es considerada como crítica.

7.1.2.3 Nombre alternativo del sujeto

La extensión "subjectAltName" es opcional y solamente se puede usar para certificados de agente electrónico de persona jurídica. En caso de ser utilizada, el uso de esta extensión debe ser "NO crítico" y únicamente está permitido el uso del nombre DNS, en concordancia con la sección 4.1.2.

7.1.2.4 Restricciones básicas

Para el caso de las CAs emisoras se debe colocar el campo "PathLenghtConstraint" con un valor de 0, para indicar que la CA no permite más sub-niveles en la ruta del certificado. Es un campo crítico.

7.1.2.5 Uso extendido de la llave

La extensión permite configurar los propósitos de la llave, y no es considerada crítica. A continuación se presenta el cuadro con los propósitos comunes:

OID	Descripción	Tipos de certificado	Obligatorio
1.3.6.1.5.5.7.3.1	Autenticación del servidor	Agente electrónico	Sí
1.3.6.1.5.5.7.3.2	Autenticación del cliente	Autenticación de persona física, Agente electrónico	Sí
1.3.6.1.5.5.7.3.4	Correo seguro	Firma de persona física, Sello electrónico	Sí
1.3.6.1.5.5.7.3.8	Estampado de tiempo (Impresión de fecha)	Estampado de tiempo	Sí
1.3.6.1.4.1.311.20.2.2	Inicio de sesión de tarjeta inteligente	Autenticación de persona física	No

7.1.2.6 Puntos de distribución de los CRL

La extensión "CRL Distribution Points" contiene las direcciones URL de la localización donde las partes que confían pueden obtener el CRL para verificar el estado del certificado. La extensión NO es crítica.

7.1.2.7 Identificador de llave de Autoridad

El método para la generación del identificador está basado en la llave pública de la CA emisora del certificado, de acuerdo a lo descrito por el RFC 3280 "Internet X.509 Public Key Infraestructura Certificate and CRL Profile". La extensión NO es crítica.

7.1.2.8 Identificador de la llave del sujeto

La extensión no es crítica, y el método para la generación del identificador de llave está basado en la llave pública del sujeto del certificado y es calculado de acuerdo con uno de los métodos descritos en el RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

7.1.3 Identificadores de objeto de algoritmos

Los certificados generados dentro de la jerarquía nacional de certificadores registrados deben usar uno de los siguientes algoritmos:

- sha256WithRSAEncryption OID::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} (Secure Hash Algorithm 256 (SHA256) with Rivest, Shamir and Adleman (RSA) encryption)
- ecdsa-with-SHA256 OID::= {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} (Elliptic Curve Digital Signature Algorithm (DSA) coupled with the Secure Hash Algorithm 256 (SHA256) algorithm)

7.1.4 Formas del nombre

Los nombres dentro de la jerarquía nacional de certificadores registrados deben cumplir las regulaciones de la sección 3.1.1. Adicionalmente, los certificados de suscriptores generalmente deben incluir el URL donde se encuentran los términos del uso de los certificados y los acuerdos entre las partes.

7.1.5 Restricciones del nombre

Los nombres se escriben en mayúsculas y sin tildes, únicamente se debe aceptar el carácter Ñ como un caso especial para los nombres de personas físicas y jurídicas.
El código de país es de dos caracteres y se asigna de acuerdo al estándar ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".

7.1.6 Identificador de objeto de Política de Certificado

El OID de la política de certificado correspondiente a cada clase de certificado es definido acorde a la sección 1.2. El director de la DGD le corresponde la administración de los "Identificadores de Objetos" (OID) para el Sistema Nacional de Certificación Digital.

7.1.7 Uso de la extensión "Restricciones de Política" (*Policy Constraints*)

Sin estipulaciones.

7.1.8 Semántica y sintaxis de los "Calificadores de Política" (*Policy Qualifiers*)

El calificador de la política está incluido en la extensión de "certificate policies" y contiene una referencia al URL con el CP aplicable y a los acuerdos de partes que confían.

7.1.9 Semántica de procesamiento para la extensión crítica de "Políticas de Certificado" (*Certificate Policies*)

Sin estipulaciones.

7.2 Perfil de la CRL

Las listas de revocación de certificados cumplen con el RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"y contienen los elementos básicos especificados en el siguiente cuadro:

Campo	Valor o restricciones
Versión	Ver sección 7.2.1
Algoritmo de firma	Algoritmo usado para la firma del CRL, puede ser: • sha256WithRSAEncryption (OID:1.2.840.113549.1.1.11) • ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)
Emisor	Entidad que emite y firma la CRL.
Fecha efectiva	Fecha de emisión del CRL.
Siguiente actualización	Fecha para la cual es emitida la siguiente CRL. La frecuencia de emisión del CRL está acorde con lo requerido en la sección 4.9.7
Certificados revocados	Lista de certificados revocados, incluyendo el número de serie del certificado revocado y la fecha de revocación.

7.2.1 Número(s) de versión

La jerarquía nacional de certificadores registrados de certificación soporta las CRLs X.509 versión 2.

7.2.2 CRL y extensiones de entradas de CRL

Sin estipulación.

7.3 Perfil de OCSP

El servicio de validación de certificados en línea OCSP (Online Certificate Status Protocol) es una forma para obtener información reciente sobre el estado de un certificado.
El servicio OCSP que se implemente debe cumplir lo estipulado en el RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.1 Número(s) de versión

Debe cumplir al menos con la versión 1 del RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.2 Extensiones de OCSP

Sin estipulaciones.

8. Auditoría de cumplimiento y otras evaluaciones

De acuerdo con el artículo 21 de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos No. 8454, "Todo certificador registrado estará sujeto a los procedimientos de evaluación y auditoría que acuerde efectuar la DCFD o el ECA".
Adicionalmente, el artículo 24 inciso e) de ese cuerpo normativo, dispone como una función de la DCFD el "fiscalizar el funcionamiento de los certificadores registrados, para asegurar su confiabilidad, eficiencia y el cabal cumplimiento de la normativa aplicable, imponiendo, en caso necesario, las sanciones previstas en esta Ley. La supervisión podrá ser ejercida por medio del ECA, en el ámbito de su competencia".
Todas las autoridades emisoras de certificados deben ajustarse al cumplimiento de las auditorías realizadas por el ECA, las cuales permiten establecer una confianza razonable en el sistema de firma digital.
Se pueden ejecutar investigaciones y revisiones para asegurar la confianza de la jerarquía nacional de certificadores registrados, las cuales incluyen, pero no se limitan a:

- Revisión de seguridad y de prácticas, las cuales incluyen instalaciones, documentos de seguridad, declaración de prácticas de certificación, acuerdos entre las partes, política de privacidad y validación de los planes para asegurar el cumplimiento de estándares.
- El ECA es la entidad responsable de ejecutar las auditorias, de acuerdo a lo estipulado en la Ley.
- La DGD puede solicitar al ECA auditorías especiales cuando tenga sospecha de un incidente o compromiso de la CA, que ponga en riesgo la integridad del sistema.

Adicionalmente, cada CA debe implementar un programa de auditorías internas para la verificación de su sistema de gestión. Dicho programa de auditorías debe estar basado en la INTE-ISO/IEC 19011 "Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental".

8.1 Frecuencia o circunstancias de evaluación

El cumplimiento de la evaluación externa del ECA se debe ejecutar al menos una vez al año y los costos deben ser asumidos por la entidad evaluada. El ECA puede realizar evaluaciones extraordinarias de acuerdo con sus procedimientos.
El programa de auditorías internas establecerá la frecuencia o circunstancias para su realización, pero en términos generales se espera que las CA ejecuten al menos una auditoría al año.

8.2 Identidad/calidades del evaluador

El personal que ejecuta las evaluaciones para el ECA incluye:

- Experto Técnico: Persona asignada por el ECA para aportar conocimientos técnicos específicos o pericia respecto al alcance de acreditación a ser evaluado.
- Evaluador: Persona designada para ejecutar como parte de un equipo evaluador, la evaluación de un Organismo de Evaluación de la Conformidad OEC.
- Evaluador Líder: Evaluador al que le es dada la completa responsabilidad por actividades de evaluación específicas.

El ECA tiene procedimientos establecidos para determinar la competencia de cada uno de estos.
Para las auditorías internas la CA debe establecer los requisitos de competencia de sus auditores según los lineamientos de la INTE-ISO/IEC 19011 "Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental".

8.3 Relación del evaluador con la entidad evaluada

Por Ley, el ECA constituye un ente independiente e imparcial, el cual ejecutará las evaluaciones acordes a sus procedimientos.

Para las auditorías internas la CA debe seguir lo establecido en la INTE-ISO/IEC 19011 “Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental”.

8.4 Aspectos cubiertos por la evaluación

Los puntos de evaluación para cada entidad son detallados a continuación:
Auditorias de la autoridad de registro
Es obligatorio que la autoridad certificadora registrada (CA emisora) supervise las autoridades de registro y notifique cualquier excepción o irregularidad de las políticas de la jerarquía nacional de certificadores registrados, y además tome las medidas para remediarlas.
Auditorias de las CA emisoras
Las CA emisoras dentro de la jerarquía nacional de certificadores registrados deben cumplir con las políticas nacionales y con los estándares determinados, a saber:

- Ley y reglamento de firma digital,
- Políticas de la raíz para los certificados de:
- Firma digital y autenticación de persona física.
- Sello electrónico y autenticación de agente electrónico.
- INTE/ISO 21188: “Infraestructura de llave pública para servicios financieros. Estructura de prácticas y políticas” o el estándar Trust Service Principles and Criteria for Certification Authorities Version vigente – Webtrust.
- RFC 3647: “Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.

Autoridades de sellado de tiempo

- Ley y reglamento de firma digital.
- Políticas de la raíz para los certificados de:
- Autoridad de sellado de tiempo.
- RFC 3161: “Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)”.
- RFC 3628: “Policy Requirements for Time-Stamping Authorities (TSAs)”.
- Política de sellado de tiempo del sistema nacional de certificación digital

8.5 Acciones tomadas como resultado de una deficiencia

La CA debe tener procedimientos para ejecutar acciones correctivas para las deficiencias identificadas tanto en las evaluaciones externas como en las auditorías internas.

8.6 Comunicación de resultados

El ECA tiene procedimientos para la ejecución de la acreditación que incluyen la comunicación de los resultados y los procedimientos de apelación.

9. Otros asuntos legales y comercialesTarifas

9.1.1 Tarifas de emisión o renovación de certificados

La tarifa para la emisión y administración de los certificados será determinada por la CA emisora del certificado.

9.1.2 Tarifas de acceso a certificados

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados no pueden cobrar por el mantenimiento de los repositorios de certificados a las partes que confían.

9.1.3 Tarifas de acceso a información del estado o revocación

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados no pueden cobrar por el mantenimiento de las listas de revocación de certificados a las partes que confían. Sin embargo, se pueden establecer tarifas para otros servicios especializados de revocación, OCSP o sellado de tiempo.

9.1.4 Tarifas por otros servicios

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados no pueden establecer tarifas para acceder información del CP o su respectivo CPS.

9.1.5 Política de reembolso

La CA que implemente una política de reembolso debe documentarla como parte de sus políticas y publicarlas dentro de su sitio Web.

9.2 Responsabilidad financiera

9.2.1 Cobertura de seguro

De acuerdo con los artículos 12 y 13 del reglamento de firma digital, es obligatorio para los sujetos privados, mantener una caución rendida preferiblemente por medio de póliza de fidelidad, y cuyo monto será fijado por la DGD. Cuando la caución esté sujeta a vencimiento, esta debe ser renovada al menos dos meses antes de la fecha de expiración.

9.2.2 Otros activos

La CA emisora debe poseer suficientes recursos financieros para mantener sus operaciones y ejecutar sus deberes. La CA emisora debe ser razonablemente capaz de administrar el riesgo de responsabilidad para los suscriptores y partes que confían.

9.2.3 Cobertura de Seguro o garantía para entidades finales

Sin estipulaciones.

9.3 Confidencialidad de la información comercial

9.3.1 Alcance de la información confidencial

Los siguientes registros del suscriptor deben ser mantenidos confidenciales:

- Registros de solicitudes de la Autoridad Certificadora, tanto aprobados como rechazados.
- Registros de solicitud de certificados de sujeto.
- Registros de las transacciones.
- Registros de pistas de auditorías.
- Planes de contingencias y recuperación de desastres.
- Medidas de seguridad controlando las operaciones de certificados (Hardware/Software).
- Servicios de administración de certificados y servicios de enrolamiento.

9.3.2 Información no contenida en el alcance de información confidencial

No se considera información confidencial las listas de revocación ni la información del estado de los certificados.

9.3.3 Responsabilidad para proteger la información confidencial

Las CA emisoras participantes dentro de la jerarquía nacional de certificadores registrados deben asegurar a los participantes que su información no será comprometida ni divulgada a terceras partes y deben cumplir con las leyes aplicables de privacidad.

9.4 Privacidad de información personal

9.4.1 Plan de privacidad

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados deben implementar las políticas de privacidad de información, de acuerdo con las leyes vigentes. No se puede divulgar o vender información de los suscriptores a certificados o información de identificación de éstos.

9.4.2 Información tratada como privada

Cualquier información acerca de los suscriptores que no esté públicamente disponible a través del contenido del certificado emitido y servicios de CRL's debe ser tratada como información privada.

9.4.3 Información que no es considerada como privada

El tratamiento de la información que no es considerada como privada, estará sujeto a lo que dispone la normativa nacional al efecto. Únicamente se considera pública la información contenida en el certificado.

9.4.4 Responsabilidad para proteger información privada

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados deben asegurar que la información privada no puede ser comprometida o divulgada a terceras partes.

9.4.5 Notificación y consentimiento para usar información privada

La información privada no puede ser usada sin el consentimiento de las partes. En este sentido, la CA no requiere notificar a los suscriptores para usar información privada.

9.4.6 Divulgación de acuerdo con un proceso judicial o administrativo

Para divulgar información privada se requiere de una orden judicial que así lo determine y se divulga estrictamente la información solicitada por los jueces.

9.4.7 Otras circunstancias de divulgación de información

La información privada podrá ser divulgada en otras circunstancias, siempre que ésta resulte expresamente prevista por la legislación aplicable.

9.5 Derechos de propiedad intelectual

Se respetarán y reconocerán los derechos de propiedad intelectual que nazcan de las actividades y creaciones de las instituciones y terceros relacionados de conformidad con el marco normativo vigente.

9.6 Representaciones y garantías

9.6.1 Representaciones y garantías de la CA

Las CA de la jerarquía nacional de certificadores registrados deben garantizar que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión del mismo.
- No haya errores en la información que fue introducida por la entidad que aprueba la emisión del certificado.
- Los certificados reúnen los requerimientos expuestos en esta CP.
- Los servicios de revocación y el uso de los repositorios cumplen lo estipulado en este CP.

9.6.2 Representaciones y garantías de la RA

Las Autoridades de Registro (RA) deben garantizar que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión del mismo.
- No se presentan errores en la información del certificado que fue introducida por las entidades de registro.
- Que los dispositivos y materiales requeridos cumplen con lo dispuesto en este CP.

9.6.3 Representaciones y garantías del suscriptor

El suscriptor debe garantizar que:

- Cada firma digital creada usando la llave privada corresponde a la llave pública listada en el certificado.
- La llave privada está protegida y que no autoriza a personas a tener acceso a la llave privada del suscriptor.
- Toda la información suplida por el suscriptor y contenida en el certificado es verdadera.
- El certificado es utilizado exclusivamente para los propósitos autorizados.

9.6.4 Representaciones y garantías de las partes que confían

Los acuerdos de partes que confían requieren que los actores conozcan suficiente información para tomar las decisiones de aceptar el certificado.

9.6.5 Representaciones y garantías de otros participantes

Sin estipulaciones.

9.7 Renuncia de garantías

Cualquier tipo de cláusula relativa a la renuncia de garantías debe estar prevista en los acuerdos de suscriptor y de partes que confían.

9.8 Limitaciones de responsabilidad legal

Las limitaciones de responsabilidad legal deben estar previstas en forma expresa en los acuerdos de suscriptor y de partes que confían.

9.9 Indemnizaciones

La CA dentro de la jerarquía nacional de certificadores registrados debe indemnizar a los suscriptores por cualquier causa legalmente establecida, incluyendo:

- Falsedad en la información suministrada.
- Por fallas en la protección del sistema de la CA, o por el uso de sistemas no confiables.

En ambos casos, se deberá demostrar ante las autoridades correspondientes los daños y perjuicios causado por la CA.

9.10 Plazo y Finalización

9.10.1 Plazo

El CP empieza a ser efectivo después de la publicación en el repositorio y los nuevos certificados deben ser emitidos cumpliendo las políticas determinadas en la nueva versión del CP.

9.10.2 Finalización

La vigencia del CP se debe mantener hasta que todos los certificados emitidos bajo esta política hayan finalizado o hayan sido reemplazados por otros certificados emitidos bajo la nueva política.

9.10.3 Efectos de la finalización y supervivencia

Después de finalizada la vigencia del CP, la cual puede ser por cambios o modificaciones en las políticas, esta se mantendrá válida mientras existan certificados activos.

9.11 Notificación individual y comunicaciones con participantes

Se permiten las comunicaciones comerciales con los participantes, a menos de que el contrato entre las partes especifique otras cláusulas.

9.12 Enmiendas

9.12.1 Procedimiento para enmiendas

De oficio el Comité Asesor de Políticas tendrá al menos una reunión anual para evaluar los atributos del certificado, determinando la conveniencia de seguir utilizando los mismos algoritmos, longitudes de las llaves y parámetros para la generación de los certificados.
Los cambios en las políticas nacionales deben ser sometidos a consulta pública, y una vez aprobadas deben comunicarse a los participantes dentro de la jerarquía nacional de certificadores registrados.
Las modificaciones o enmiendas de las políticas deben documentarse y mantenerse actualizadas a través de versiones. Las enmiendas deben publicarse en el sitio Web de la CA emisora.

9.12.2 Mecanismo y periodo de notificación

La DGD es la responsable de realizar los comunicados a las CA emisoras para implementar las modificaciones. Al menos treinta días naturales antes de cualquier cambio mayor en las políticas, estas se deben publicar en el sitio Web y realizar una comunicación en los medios escritos.

9.12.3 Circunstancias bajo las cuales los OID deben ser cambiados

Los cambios en los OIDs corresponden a nuevas políticas que contengan otros objetos con OID adicionales. Si la estructura del certificado se mantiene entonces no es necesario cambiar los OIDs.

9.13 Disposiciones para resolución de disputas

De acuerdo con la Ley N°8454, le compete a la DGD la resolución de las disputas, como órgano administrador y supervisor del sistema de certificación digital. Las resoluciones dictadas por la DGD agotan la vía administrativa.

9.14 Ley gobernante

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados están sujetas a las leyes de la República de Costa Rica, en particular de la Ley N°8454 “Ley de certificados, firmas digitales y documentos electrónicos” y su reglamento.

9.15 Cumplimiento con la Ley aplicable

Las políticas descritas cumplen con las regulaciones nacionales.

9.16 Disposiciones varias

9.16.1 Acuerdo completo

No aplicable.

9.16.2 Asignación

No aplicable.

9.16.3 Separabilidad

En el eventual caso que una cláusula de la política sea declarada inconstitucional por los tribunales de justicia o las leyes, el resto de las cláusulas de estas políticas se mantendrán vigentes.

9.16.4 Aplicación (Honorarios de abogado y renuncia de derechos)

No aplicable.

9.16.5 Fuerza mayor

Los acuerdos de suscriptores y partes que confían deben incluir cláusulas de fuerza mayor para proteger a la CA emisora.

9.17 Otras disposiciones

No aplicable.

Anexo A: Documentos de referencia

Los siguientes documentos referenciados son aplicados para la confección de las políticas de certificación.

- RFC 3039 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile.

- RFC 3280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.
- RFC 3647: “Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.
- RFC 3161: “Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)”.
- RFC 3628: “Policy Requirements for Time-Stamping Authorities (TSAs)”.
- INTE-ISO-21188:2007 “Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas.
- INTE-ISO/IEC 19011 “Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental”.
- ISO 3166 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países.
- INTE-ISO/IEC 17021 Evaluación de la conformidad — Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión.
- Ley N°8454 “Ley de certificados, firmas digitales y documentos electrónicos” y su reglamento.

Documentos anexos:

- Política de sellado de tiempo del sistema nacional de certificación digital.
- Directrices para las Autoridades de Registro. Características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica.
- Guía para la autorización de una Autoridad Certificadora Emisora de la jerarquía nacional de certificadores registrados de Costa Rica.