Camerfirma PERÚ

Tinexta Infocert

PUB-2025-14-05
Política de certificación - EC

Contenido

1. Tratamiento del documento

1.1. Control de actualizaciones

VERSIÓN	FECHA	ELABORADO	APROBADO
1.0	Agosto 2022	Innovate DC	Ramiro Muñoz
1.1	Julio 2023	Innovate DC	Marta Ortega
2.0	Diciembre 2025	Adrián Sastre	Julio César Infante

1.2. Control de cambios

DESCRIPCION DEL CAMBIO	APARTADOS QUE CAMBIAN RESPECTO A VERSIÓN ANTERIOR
AÑADIDO	
MODIFICADO	Actualización de formato corporativo. Se incorporan los perfiles de firma remota.
ELIMINADO	

1.3. Mantenimiento del documento

Se requiere mantenimiento y/o revisión de este documento, cada vez que varíen algunas de las fases del proceso, las funciones del personal involucrado o las herramientas utilizadas en el mismo

1.4. Validez

Hasta su actualización.

Cualquier copia local se considera una **copia no controlada**. Es responsabilidad de quienes utilizan copias no controladas verificar su nivel de actualización.

1.5. Tratamiento y confidencialidad

Documento de uso público, pudiendo acceder a él todas las partes interesadas a través de la página web.

1.6. Distribución

Distribución pública.

2. Introducción

2.1. Consideración inicial

Por no haber una definición taxativa de los conceptos de Declaración de Prácticas de Certificación (DPC o CPS) y Políticas de Certificación (PC) y debido a algunas confusiones formadas, entendemos que es necesario aclarar dichos conceptos.

Política de Certificación es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad o en alguna aplicación, con requisitos de seguridad y utilización comunes, es decir, en general una Política de Certificación debe definir la aplicabilidad de tipos de certificado para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

La Declaración de Prácticas de Certificación es definida como un conjunto de prácticas adoptadas por una Entidad de Certificación (EC) para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Titular, el Firmante, la Parte Usuaria que confía y la Entidad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

Estos conceptos de Políticas de Certificación y Declaración de Prácticas de Certificación son distintos, pero aun así es muy importante su interrelación.

Una DPC detallada no forma una base aceptable para la interoperabilidad de Entidades de Certificación. Las Políticas de Certificación sirven mejor como medio en el cual basar estándares y criterios de seguridad comunes.

En definitiva, una política define “qué” requerimientos de seguridad son necesarios para la emisión de los certificados. La DPC nos dice “cómo” se cumplen los requerimientos de seguridad impuestos por la política.

2.2. Vista general

El presente documento especifica la Política de Certificación de las siguientes categorías de certificados:

- Certificado de Persona Jurídica – Atributo de Vinculación a Entidad.
- Certificado de Persona Jurídica – Atributo de Representante Legal.
- Certificado de Persona jurídica (sin atributo).
- Certificado de Persona Jurídica – Atributo de Facturación Electrónica.
- Certificado de Persona Natural
- Certificado de Persona Natural – Profesional Colegiado
- Certificado de Sello Electrónico de Empresa / Agente automatizado

Esta PC está basada en la especificación del estándar RCF 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, de IETF.

Esta Política de Certificación está en conformidad con las disposiciones legales que rigen el asunto de Firma Electrónica y Certificación electrónica en Perú, cumpliendo todos los requisitos técnicos y de seguridad exigidos para la emisión de certificados cualificados.

Esta política define las reglas y responsabilidades que deben seguir aquellas Entidades de Certificación que deseen emitir los tipos de certificados definidos en el presente documento, imponiendo además ciertas obligaciones que deben ser tenidas en cuenta por los Titulares, Firmantes y Partes Usuarias que confían en virtud de su especial relación con este tipo de certificados.

De esta forma, cualquier EC que emita este tipo de certificados, deberá ajustarse a los niveles de seguridad que se detallan en esta política de certificación y deberán informar a sus Titulares y Firmantes de su existencia.

Los certificados emitidos bajo esta política requerirán la autenticación de la identidad de los Firmantes. Esta identificación y autentificación se realizará según los términos de esta PC.

La EC suspenderá y revocará sus certificados según lo dispuesto en esta PC.

La EC deberá conservar los registros e incidencias de acuerdo con lo que se establece en esta PC. Las funciones críticas del servicio deberán ser realizadas al menos por dos personas.

Las claves de los Firmantes tienen un periodo de validez determinado por esta PC y en ningún caso podrán realizarse copias de back-up, ni almacenarse por la EC, salvo por lo expresamente permitido por las normas aplicables.

La información personal recabada del Firmante se recogerá con el debido consentimiento del interesado y únicamente para los fines propios del servicio de certificación, el cual podrá ejercitar en todo caso sus oportunos derechos de información, rectificación y cancelación. La EC deberá respetar así mismo la normativa aplicable en materia de protección de datos aplicable en Perú: Ley nº29733 de Protección de Datos Personales y su Reglamento (Decreto Supremo 016-2024 JUS).

La actividad de la EC podrá ser sometida a la inspección de la Autoridad de la Políticas (PA) o por personal delegado por la misma.

En lo que se refiere al contenido de esta PC, se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto. En la página web de Camerfirma (www.camerfirma.com.pe) hay algunas informaciones útiles.

2.3. Identificación

La presente PC está identificada con los siguientes OID:

Certificado	OID Políticas
Certificado de Persona Jurídica – Atributo de Vinculación a Entidad	[Camerfirma] 1.3.6.1.4.1.17326.30.16.0.1 (en software) 1.3.6.1.4.1.17326.30.16.0.2 (en tarjeta) 1.3.6.1.4.1.17326.30.16.0.3 (en nube)

Certificado de Persona Jurídica – Atributo de Representante Legal	1.3.6.1.4.1.17326.30.16.10.1 (en software) 1.3.6.1.4.1.17326.30.16.10.2 (en tarjeta)
Certificado de Persona jurídica (sin atributo)	1.3.6.1.4.1.17326.30.16.20.1 (en software) 1.3.6.1.4.1.17326.30.16.20.2 (en tarjeta)
Certificado de Persona Jurídica – Atributo de Facturación Electrónica	1.3.6.1.4.1.17326.30.16.30.1 (en software) 1.3.6.1.4.1.17326.30.16.30.2 (en tarjeta)
Certificado de Persona Natural	1.3.6.1.4.1.17326.30.16.40.1 (en software) 1.3.6.1.4.1.17326.30.16.40.2 (en tarjeta)
Certificado de Persona Natural – Profesional Colegiado	1.3.6.1.4.1.17326.30.16.60.1 (en software) 1.3.6.1.4.1.17326.30.16.60.2 (en tarjeta)
Certificado de Sello Electrónico de Empresa / Agente automatizado	1.3.6.1.4.1.17326.30.16.50.1 (en software) 1.3.6.1.4.1.17326.30.16.50.2 (en tarjeta)

2.4. Comunidad y ámbito de aplicación

2.4.1. Entidad de Certificación (EC)

Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Firmante y la Parte usuaria que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una persona (Firmante), relacionada en su caso a una entidad concreta (Persona Jurídica), a través de la emisión de un Certificado.

El emisor de este tipo de certificados es Camerfirma Perú S.A.C.

2.4.2. Entidad de Registro (ER)

Ente que actúa conforme esta Política de Certificación y, en su caso, mediante acuerdo suscrito con la EC, cuyas funciones son la gestión de las solicitudes, identificación y registro y verificación de los solicitantes del Certificado y aquellas que se dispongan en las Prácticas de Certificación concretas.

2.4.3. Firmante o titular de la firma

Bajo esta Política el Firmante o Titular del certificado es el responsable de los efectos jurídicos generados por la utilización de una firma digital. Tratándose de personas naturales, éstas son firmantes/titulares del certificado y de las firmas digitales que se generen a partir de aquél. En el caso de personas jurídicas, son éstas las titulares del certificado digital, y sus representantes o personas vinculadas, los suscriptores poseedor y responsable de la generación y uso de las claves, salvo el caso de las firmas digitales que generen a través de agentes automatizados para las cuales las personas jurídicas son titulares de los certificados y de las firmas digitales generadas a partir de éstos.

Tipo de certificado	Firmante/Titular
Persona Jurídica – Atributo de Vinculación a Entidad	Persona Jurídica que faculta a una persona natural de atributo limitado de vinculación a una Entidad en virtud de una relación laboral o mercantil, para poder actuar en nombre de la persona jurídica de forma limitada (atributo limitado).
Persona Jurídica – Atributo Representante Legal	Persona Jurídica que faculta a una persona natural de atributo de representante legal de una Entidad o apoderado general, para poder actuar en nombre de la persona jurídica de forma plena (atributo pleno).
Persona Jurídica (sin atributo)	Persona Jurídica titular del certificado para usos donde no se necesita firma de persona natural.
Persona Jurídica – Atributo de Facturación Electrónica	Persona Jurídica que faculta a una persona natural de atributo exclusivo para la realización de Facturación electrónica en nombre de la persona jurídica (atributo limitado).
Persona Natural / Persona Natural – Profesional Colegiado	Persona Natural
Sello electrónico / Agente automatizado	Persona Jurídica Titular del certificado

2.4.4. Parte usuaria que confía

En esta Política se entiende por Parte Usuaria que confía la persona que voluntariamente confía en el certificado emitido a favor del emisor, lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado y en consecuencia se sujeta a lo dispuesto en esta Política, por lo que no se requerirá acuerdo posterior alguno.

La Parte Usuaria que confía también puede denominarse como “Tercero que Confía”.

2.4.5. Solicitante o suscriptor

Se entenderá por Solicitante la persona física que solicita el Certificado y que podrá ser considerada como Suscriptor del Certificado. Podrán solicitar los certificados las siguientes personas físicas:

Tipo de certificado	Solicitante / Suscriptor
Persona Jurídica – Atributo de Vinculación a Entidad	Persona natural vinculada a una determinada Entidad y facultada para actuar en nombre de la persona jurídica de forma limitada (como empleado, funcionario, colaborador, colegiado…)
Persona Jurídica – Atributo de Representante Legal	Persona natural facultada para actuar en nombre de la persona jurídica de forma plena y sin limitaciones (como Gerente General, administrador, representantes legales o

Tipo de certificado	Solicitante / Suscriptor
	voluntarios de la Entidad con poderes generales).
Persona Jurídica (sin atributo)	Persona natural autorizada para solicitar el certificado por la persona jurídica titular del certificado y utilizarlo para usos que no requiere firma de persona natural.
Persona Jurídica – Atributo de Facturación electrónica	Persona natural facultada para actuar en nombre de la persona jurídica para la realización de Facturación electrónica exclusivamente.
Persona Natural / Persona Natural – Profesional Colegiado	Persona natural Titular del certificado
Sello electrónico / Agente automatizado	Persona natural con representación u autorización de la Entidad Titular del certificado para su uso.

2.4.6. Entidad

A efectos de la presente Política de Certificación nos referiremos a una Entidad como aquella empresa u organización de cualquier tipo. Siempre que la norma aplicable lo permita, la Entidad podría tener o no personalidad jurídica, aunque en esta Política nos referimos únicamente a la Entidad como a una Organización con personalidad jurídica:

Tipo de certificado	Entidad
Persona Jurídica – Atributo de Vinculación a Entidad	Organización con personalidad jurídica, a la cual pertenece o a la que se encuentra estrechamente vinculado el Suscriptor, incluyendo a los empresarios individuales. La Entidad deberá solicitar la suspensión/revocación del certificado cuando cese la vinculación del Suscriptor con la organización o se revoquen sus facultades de representante legal.
Persona Jurídica – Atributo de Representante Legal	Organización con personalidad jurídica, de cualquier tipo en la que el Suscriptor actúa como representante legal. La Entidad deberá solicitar la suspensión/revocación del certificado cuando cese la capacidad de representación o el apoderamiento que ostenta el Suscriptor.
Persona Jurídica (sin atributo)	Organización con personalidad jurídica que actúa como titular del certificado. El Solicitante/Suscriptor o el representante legal, deberá solicitar la suspensión/revocación del certificado cuando lo estime procedente o cuando desaparezca la Entidad
Persona Jurídica – Atributo de Facturación electrónica	Organización con personalidad jurídica que actúa como titular del certificado.

Tipo de certificado	Entidad
	La Entidad deberá solicitar la suspensión/revocación del certificado cuando cese la capacidad del Suscriptor de realizar Facturación electrónica para la entidad.
Persona Natural / Persona Natural – Profesional Colegiado	-----
Sello electrónico / Agente automatizado	Organización con personalidad jurídica que actúa como titular del certificado. El Suscriptor o el representante legal, deberá solicitar la suspensión / revocación del certificado cuando lo estime procedente o cuando desaparezca la Entidad

2.4.7. Ámbito de aplicación y usos

Tipo de certificado	Ámbito de Aplicación
Persona Jurídica – Atributo de Vinculación a Entidad	Identificar a una Persona Jurídica (Titular/Firmante) y a la Persona Natural (Suscriptor) que mantiene una vinculación con la Entidad , de carácter laboral, mercantil u otro, y permite evidenciar el no repudio de sus acciones dentro de sus facultades limitadas (atributo limitado).
Persona Jurídica- Atributo Representante Legal	Identificar a una Persona Jurídica (Titular/Firmante) y a la Persona Natural (Suscriptor) física que tiene facultades de representación de la Persona Jurídica y permite evidenciar el no repudio de sus acciones dentro de sus facultades con plenos poderes (atributo pleno)
Persona Jurídica	Certificado que identifica a una Persona Jurídica y que generalmente está asociado a una clave activada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves se asocia al uso de un certificado de sello electrónico dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se permite usarse como elemento de identificación cliente de maquina en protocolos de comunicación seguros TLS.
Persona Jurídica – Atributo de Facturación electrónica	Certificado exclusivo para la realización de facturas electrónicas a nombre de una Entidad. La acción de las claves se asocia al uso de un certificado de vinculación dota de integridad y autenticidad a las facturas sobre los que se aplica.
Persona Natural	Determina la identidad de la persona natural firmante para actuar en su propio nombre.
Persona Natural – Profesional Colegiado	Determina la identidad de la persona natural firmante para actuar en su propio nombre así como su situación de profesional colegiado dado de alta en un determinado Colegio profesional del Perú (colegiatura activa)

Tipo de certificado	Ámbito de Aplicación
Sello electrónico / Agente automatizado	Este certificado puede estar asociado a una clave activada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves se asocia al uso de un certificado de sello electrónico dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se permite usarse como elemento de identificación cliente de maquina en protocolos de comunicación seguros TLS.

Todos los certificados emitidos bajo esta Política son válidos para asumir responsabilidades, compromisos o derechos en su propio nombre, y en el caso de los certificados que impliquen vinculación con una Entidad, también en nombre de la entidad en la medida en que se deduzca y dentro del ámbito concreto de ese vínculo.
Los Certificados emitido bajo esta Política pueden ser utilizados con los siguientes propósitos:

- Identificación del Firmante: El Firmante puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.

  El Firmante podrá identificarse válidamente ante cualquier persona mediante la firma de un e-mail o cualquier otro tipo de datos.

- Integridad del documento firmado: La utilización del Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Firmante. Se certifica que el mensaje recibido por la Parte Usuaria que confía es el mismo que fue emitido por el Firmante.

- No repudio de origen: Con el uso de este Certificado también se puede garantizar que el Firmante se compromete con los datos asociados a la firma electrónica, generándose una evidencia suficiente para demostrar la autoría de los datos asociados, y su integridad.

Usos prohibidos y no autorizados

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso.

El empleo de los certificados que implique la realización de operaciones no autorizadas según las PC aplicables a cada uno de los Certificados, la DPC y los Contratos de la EC con sus Firmantes tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la EC, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el Firmante o cualquier tercero.

En función de los servicios prestados por la EC mediante la emisión de sus certificados, no es posible por parte de la EC el acceso o conocimiento del contenido del mensaje al que haya sido adjuntado o con el que se relacione el uso de un certificado emitido por la EC.

Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la EC emitir valoración alguna sobre dicho contenido, asumiendo por tanto el Firmante cualquier responsabilidad dimanante del contenido de dicho mensaje aparejado al uso de un certificado emitido por la EC. Asimismo, le será imputable al Firmante cualquier responsabilidad que

pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en las PC aplicables a cada uno de los Certificados, la DPC y los contratos de la EC con sus Firmantes, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

2.5. Contacto

La presente política de certificación está administrada y gestionada por el Departamento Jurídico de AC Camerfirma SA, pudiendo ser contactado por los siguientes medios:

- Email: juridico@camerfirma.com
- Teléfono: +34 902 361 207
- Dirección: C/ Rodríguez Marín Nº88 – 28016 (Madrid)
- Localización: https://www.camerfirma.com.pe/usuarios/

3. Cláusulas generales

3.1. Obligaciones

3.1.1. EC

Las EC's que actúan bajo esta Política de Certificación estarán obligadas a cumplir con lo dispuesto por la normativa vigente y además a:

1. Respetar lo dispuesto en esta Política.
2. Proteger sus claves privadas de forma segura.
3. Emitir certificados conforme a esta Política y a los estándares de aplicación.
4. Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos
5. Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados cualificados.
6. Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
7. Suspender y revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL
8. Informar a los Firmantes de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.
9. Publicar esta Política y las Prácticas correspondientes en su página web.
10. Informar sobre las modificaciones de esta Política y de su DPC a los Suscriptores y ER's que estén vinculadas a ella y/o que comercialicen sus certificados.
11. No almacenar ni copiar los datos de creación de firma del Firmante, en caso de su gestión en nombre de éste.
12. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.
13. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante perdida o destrucción o falsificación.
14. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

3.1.2. ER

Las ER's que actúen bajo esta Política de Certificación estarán obligadas a cumplir con lo dispuesto por la normativa vigente y además a:

1. Respetar lo dispuesto en esta Política.
2. Proteger sus claves privadas.
3. Comprobar la identidad de los Solicitantes de certificados.
4. Verificar la exactitud y autenticidad de la información suministrada por el Firmante solicitante.
5. Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Firmante.
6. Respetar lo dispuesto en los contratos firmados con la EC y con el Firmante.
7. Informar a la EC de las causas de revocación, siempre y cuando tomen conocimiento.

3.1.3. Solicitante/Suscriptor

El Solicitante/Suscriptor de un Certificado deberá cumplir con lo dispuesto por la normativa aplicable y además deberá:

1. Suministrar a la ER la información necesaria para realizar una correcta identificación del Firmante y de la Entidad.
2. Demostrar ser poseedor de facultades de representación legal, poderes generales o poderes especiales que le permiten actuar en nombre de la Entidad en el ámbito de sus facultades vigentes.
3. Confirmar la exactitud y veracidad de la información suministrada.
4. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
5. Asumir las Obligaciones del Firmante/Titular para los certificados de Persona Jurídica – Atributos, Persona Jurídica y Sello electrónico.

3.1.4. Firmante/Titular

El Firmante/Titular de un certificado estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

1. Custodiar su clave privada de manera diligente.
2. Usar el certificado según lo establecido en la presente Política de Certificación.
3. Respectar lo dispuesto en el contrato firmado con la Entidad de Certificación.
4. Informar de la existencia de alguna causa de suspensión /revocación.
5. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

3.1.5. Parte usuaria que confía

Será obligación de la Parte Usuaria que confía cumplir con lo dispuesto por la normativa vigente y:

1. Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos y consultar sobre la revocación de los certificados a través de la publicación CRL disponible en https://www.camerfirma.com.pe/usuarios/
2. Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.
3. No usar los certificados fuera de los términos establecidos en el marco de la IOFE.

3.1.6. Entidad

En caso de Certificados de Persona Juridica – Atributo de Representante Legal y de vinculación a Entidad será obligación de la Entidad solicitar a la ER la suspensión / revocación del certificado cuando cese la capacidad de representación que ostenta el Firmante o cuando cese o se modifique la vinculación del Firmante con la Entidad.

3.1.7. Repositorio

La información relativa a la publicación y revocación /suspensión de los certificados se mantendrá accesible al público en los términos establecidos en la normativa vigente.

La EC deberá mantener un sistema seguro de almacén y recuperación de certificados y un repositorio de certificados revocados, pudiendo delegar estas funciones en una tercera entidad.

3.2. Responsabilidad

La EC dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente. Siendo filial de AC Camerfirma, S.A., podrá beneficiarse de las Pólizas contratadas por su matriz.

La EC actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los certificados, de los signatarios y de los terceros que confíen en los certificados.

Las responsabilidades de la EC incluyen las establecidas por la presente Política de Certificación, así como las que resulten de aplicación como consecuencia de la normativa española e internacional.
La EC será responsable del daño causado ante el Firmante o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

1. la exactitud de toda la información contenida en el certificado en la fecha de su emisión.
2. la garantía de que, en el momento de la entrega del certificado, obra en poder del responsable de la entidad, la clave privada correspondiente a la clave pública dada o identificada en el certificado.
3. la garantía de que la clave pública y privada funcionan conjunta y complementariamente.
4. la correspondencia entre el certificado solicitado y el certificado entregado.
5. cualquier responsabilidad que se establezca en cada momento por la legislación vigente.

3.2.1. Exoneración de responsabilidad

Las EC's y las ER's no serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
2. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Certificación.
3. Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Autoridad de Certificación.
4. Por el uso de la información contenida en el Certificado o en la CRL.
5. Por el incumplimiento de las obligaciones establecidas para el Firmante, el Responsable de la Entidad o Parte Usuaria que confía en la normativa vigente, la presente Política de Certificación o en las Prácticas Correspondientes.

6. Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
7. Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
8. Por la no recuperación de documentos cifrados con la clave pública del Firmante.
9. Fraude en la documentación presentada por el solicitante.
10. La EC no se responsabiliza del contenido ni del alcance de los poderes notariales del representante de la entidad, Firmante del certificado.

3.2.2. Límite de responsabilidad en caso de pérdidas por transacciones

Independientemente del importe de las transacciones, este tipo de certificados tienen un límite de responsabilidad igual a 0 soles.

Esta garantía será de aplicación a efectos de lo dispuesto en la legislación vigente.

3.3. Responsabilidad financiera

La EC no asume ningún tipo de responsabilidad financiera.

3.4. Interpretación y ejecución

3.4.1. Legislación

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por lo dispuesto en la legislación peruana, así como por la legislación española y comunitaria vigente en cada momento, siempre y cuando éstas no contradigan la legislación peruana.

3.4.2. Independencia

La invalidez de una de las cláusulas contenidas en esta Política de Certificación no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

3.4.3. Notificación

Cualquier notificación referente a la presente Política de Certificación se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

3.4.4. Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte de Arbitraje de la Cámara Oficial de Comercio de España en el Perú, y en su defecto al Centro de Arbitraje de la Cámara de Comercio de Lima (CCL) de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

3.5. Tarifas

3.5.1. Tarifas de emisión de certificados y re-emisiones

Los precios de los servicios de certificación o cualesquiera otros servicios relacionados estarán disponibles para las Partes Usuarias en la página web de Camerfirma www.camerfirma.com.pe y / o en la de cada ER concreta.

3.5.2. Tarifas de acceso a los certificados

El acceso a los certificados emitidos es gratuito, no obstante, la EC se reserva el derecho de imponer alguna tarifa para los casos de descarga masiva de CRLs o cualquier otra circunstancia que a juicio de la EC deba ser gravada.

3.5.3. Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

La EC proveerá de un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito.

3.5.4. Tarifas de acceso al contenido de estas políticas de certificación

El acceso al contenido de la presente Política de Certificación será gratuito.

3.5.5. Política de reintegros

La EC dispondrá de una política de reintegros puesta a disposición de las Partes Usuarias en la dirección de Internet https://www.camerfirma.com.pe y / o en la de cada ER concreta.

No se podrá reintegrar el precio de un certificado ya emitido, aunque el solicitante no lo haya descargado, salvo en los supuestos indicados en el punto 4.4.

3.6. Publicación y repositorios

3.6.1. Publicación de información de la AC

Políticas y prácticas de certificación

La EC estará obligada a publicar la información relativa a sus Políticas y Prácticas de Certificación.
La presente Política de Certificación es pública y se encuentra disponible en el sitio de Internet https://www.camerfirma.com.pe

Las Prácticas de Certificación de referencia serán así mismo públicas y se pondrán a disposición del público en la dirección de Internet https://www.camerfirma.com.pe

Términos y condiciones

La EC o la ER pondrán a disposición de los Firmantes y Partes Usuarias los términos y condiciones del servicio antes de proceder a la emisión del certificado o de entregar los PINES o claves que permitan el acceso a la clave privada.

Difusión de los certificados

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son accesibles para los Firmantes y las Partes Usuarias.

En concreto:

a) El certificado de la EC es público y se encontrara disponible en la página web de Camerfirma www.camerfirma.com.pe
b) El resto de los certificados estarán disponibles al público en la página web de Camerfirma Perú sólo en los casos en que el Firmante haya otorgado su consentimiento
c) La EC pondrá a disposición de las Partes Usuarias los términos y condiciones referentes al uso de los certificados
d) La información a la que se refieren los puntos a) y b) estará disponible 24 horas al día, 7 días por semana. En caso de fallo del sistema u otros factores que no se encuentran bajo el control de la EC, la EC hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

3.6.2. Frecuencia de publicación

Las Políticas y Prácticas de Certificación se publicarán una vez hayan sido creadas o en el momento en que se apruebe una modificación de las mismas.

La EC publicará los certificados suspendidos en el momento en que reciba una petición autenticada y existan indicios de su necesidad.

La CRL que contiene la lista de los certificados revocados se publicará con una frecuencia mínima diaria.

3.6.3. Controles de acceso

El acceso a la información será gratuito y estará a disposición de los Firmantes y las Partes Usuarias. La EC podrá establecer sistemas de seguridad para controlar el acceso a la información contenida en el web, LDAP o CRL con el fin de evitar usos indebidos que afecten a la protección de datos personales.

3.7. Auditorías

3.7.1. Frecuencia de las auditorías

Se realizará una auditoría interna con una periodicidad mínima anual, y una auditoria de seguimiento realizada por la Autoridad Administrativa Competente (INDECOPI) también anual, salvo que se establezca un plazo menor por la normativa vigente. En dichas auditorias se revisarán los registros, archivos, procedimientos y controles aplicados por la EC.

3.7.2. Identificación y calificación del auditor

El auditor debe poseer conocimientos y experiencia en sistemas de PKI y en seguridad de sistemas informáticos. Para las evaluaciones de seguimiento y renovación de EC y ER el Auditor debe ser autorizado por el INDECOPI, y no haber realizado trabajos para ella dentro de los 2 años anteriores a la ejecución de la auditoría.

3.7.3. Relación entre el auditor y la EC

La auditoría deberá ser realizada por un auditor independiente y neutral.

Lo anterior no impedirá la realización de auditorías internas periódicas.

3.7.4. Tópicos cubiertos por la auditoría

La auditoría deberá verificar en todo caso:

a) Que la EC tiene un sistema que garantice la calidad del servicio prestado.
b) Que la EC cumple con los requerimientos de esta Política de Certificación.
c) Que las Prácticas de Certificación de la EC se ajustan a lo establecido en esta Política, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.

3.7.5. Auditoría en las entidades de registro

Todas las Entidades de Registro deben ser auditadas al ser estas entidades delegadas de actividades responsabilidad de la EC. Estas auditorías se realizarán como mínimo cada año y podrán ser realizadas por la propia EC o por una entidad externa.

3.8. Confidencialidad

3.8.1. Tipo de información a mantener confidencial

Se determinará por la EC la información que deba ser considerada confidencial, debiendo cumplir en todo caso con la totalidad de la normativa vigente en materia de protección de datos.

La EC pondrá todos los medios a su alcance para garantizar la confidencialidad frente a terceros, durante el proceso de generación, de las claves privadas de firma digital que proporciona. Asimismo, una vez generadas y entregadas las claves privadas, la EC se abstendrá de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir dichas claves, salvo expresa disposición legal en sentido contrario.

3.8.2. Tipo de información considerada no confidencial

Se considerará como información no confidencial:

a) La contenida en la presente Política y en las Prácticas de Certificación.
b) La información contenida en los certificados siempre que el Firmante haya otorgado su consentimiento.
c) Cualquier información cuya publicidad sea impuesta normativamente.
d) Las que así se determinen por las Prácticas de Certificación siempre que no contravengan ni la normativa vigente ni lo dispuesto en esta Política de Certificación.

3.8.3. Divulgación de información de revocación/suspensión de certificados

La forma de difundir la información relativa a la suspensión o revocación de un certificado se realizará mediante la publicación de las correspondientes CRLs.

3.8.4. Envío a la autoridad competente

Se proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

3.9. Derechos de propiedad intelectual

La EC es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta Política de Certificación. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la EC sin la autorización expresa por su parte. No obstante, no necesitará autorización de la EC para la reproducción del Certificado cuando la misma sea necesaria para su utilización por parte la Parte Usuaria que confía legítima y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta Política de Certificación.

4. Identificación y autenticación

4.1. Registro inicial

4.1.1. Tipos de nombres

Todos los Firmantes/Suscriptores requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500.

4.1.2. Pseudónimos

Se podrán usar pseudónimos siempre y cuando lo permita la norma aplicable en cada momento en la jurisdicción de la EC.

4.1.3. Reglas utilizadas para interpretar varios formatos de nombres

Se atenderá en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

Se permite el uso dentro del CN del uso de un ACRÓNIMO que identifique a la Entidad a la que está vinculada el titular del certificado. Esta alternativa es importante cuando un titular posee más de un certificado debido a su vinculación a más de una empresa. Algunos aplicativos solo muestran el nombre del titular a la hora de elegir un certificado del almacén para realizar un proceso de autenticación o firma. En estos casos el titular no tiene una forma rápida de diferenciar el certificado a usar.

El formato del CN dentro del certificado será:
“Nombre del Titular [ACRÓNIMO]”

4.1.4. Unicidad de los nombres

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los nombres de los certificados emitidos. El atributo del SerialNumber se usará para distinguir entre dos DN’s similares. La EC es responsable de realizar los esfuerzos que razonablemente estén a su alcance para asegurar que el SerialNumber es suficiente para resolver las posibles colisiones entre nombres.

4.1.5. Procedimiento de resolución de disputas de nombres

Se atenderá a lo dispuesto en el apartado 2.4.4 de este documento

4.1.6. Reconocimiento, autenticación y función de las marcas registradas

Se admitirá la identificación de marcas o acrónimos de entidades siempre que en el propio certificado aparezca, además, la razón social y el número de identificación fiscal de la Entidad u otro elemento de identificación inequívoco, como el número de identificación fiscal, titular del signo distintivo registrado o no. La EC no asumirá ninguna responsabilidad respecto del uso de marcas u otros signos distintivos, registrados o no, en la emisión de los Certificados expedidos bajo la presente Política de Certificación.

4.1.7. Métodos de prueba de la posesión de la clave privada

Si el par de claves es generado por el Firmante, la EC proveerá en la DPC la garantía de estar en posesión de clave privada. En caso contrario, la EC deberá tomar las medidas necesarias que aseguren que el Firmante está en posesión de la clave privada asociada a la clave pública.

4.1.8. Autenticación de la identidad de una organización

En el caso de los certificados emitidos bajo la presente Política donde se incorporen los datos de una persona jurídica, se exigirá, en todo caso, la acreditación de la existencia de la Entidad por un medio conforme al Derecho aplicable a la nacionalidad de la entidad.
Además, la identidad de la persona jurídica se verificará:

- En el caso de empresas con domicilio en Perú, la existencia y vigencia de la persona jurídica deberá acreditarse con el documento o consulta electrónica de vigencia emitidos por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente, se debe verificar también mediante la base de datos de SUNAT que el RUC se encuentre activo y habido.
- En empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente o consulta en línea expedida por la autoridad competente en su país de origen.

4.1.9. Autenticación de la identidad del firmante

Métodos de identificación: Para realizar una correcta identificación de la identidad del Solicitante/Firmante/Suscriptor, se deberá atender a lo dispuesto por la legislación vigente.

En los certificados emitidos bajo esta Política, para realizar una correcta identificación de la identidad del Firmante, se deberá atender a lo dispuesto por la legislación vigente en cada momento.

En concreto, en el momento de elaboración de la presente versión de esta PC, en base a la Segunda Disposición Complementaria Modificatoria del Decreto Supremo N° 029-2021-PCM, publicado el 19 de febrero de 2021, para los certificados catalogados como cualificados o emitidos dentro de la IOFE, la identificación y la comprobación de la información brindada por los titulares y/o suscriptores del certificado digital debe efectuarse:

- en presencia física del solicitante, o
- a distancia, mediante el uso de los certificados digitales del solicitante entregados en su Documento Nacional de Identidad electrónico o digital, o

- a distancia, utilizando métodos de identificación aprobados por la Autoridad Administrativa Competente que provean una seguridad equivalente en términos de fiabilidad a la presencia física."

En situaciones excepcionales como la pandemia originada por el Covid-19, y siempre y cuando lo autorice previamente la Autoridad Administrativa Competente (INDECOPI), se podrán habilitar otros métodos de identificación que permiten asegurar un nivel de seguridad equivalente a la presencia física, como la Video identificación.

Documentos acreditativos: La identidad se acreditará mediante la presentación de un documento válido de identidad como el DNI, la tarjeta de residente o el pasaporte.

Esta información deberá incorporarse en el certificado en las extensiones destinadas a los nombres alternativos del titular del certificado (Subject Alt Name).

4.1.10. Autenticación de las facultades de representación del firmante

Para los Certificados de Persona Jurídica – Atributo de Representante Legal, emitidos bajo esta Política se exige, además, la comprobación de la extensión y vigencia de las facultades de representación del Firmante.

4.1.11. Autenticación del vínculo existente entre la entidad y el firmante

Para los Certificados de Persona Jurídica -Atributo de vinculación a Entidad, se deberán comprobar y documentar la vinculación entre la Entidad y el Firmante mediante la presentación de los documentos oficiales correspondientes u autorización específica otorgada por una persona con poder de representación de la entidad, de conformidad con su normativa específica.

Modelo orientativo de poderes

La EC (por si misma o a través de la ER) deberá verificar que el Firmante dispone de poderes notariales con un contenido mínimo que le permita asumir la realización de ciertos actos en nombre de la entidad a la que representa. No obstante, lo anterior, el contenido y alcance concreto de dichos poderes deberá ser verificado por la Parte Usuaria que confía antes de depositar su confianza en el certificado, en función del negocio jurídico subyacente en la transacción electrónica.

Certificado de Representante

El poder notarial del Firmante podrá contener, de forma orientativa, las siguientes menciones:

a) Administrar, bienes muebles e inmuebles, ejercitar y cumplir toda clase de derechos y obligaciones; rendir, exigir y aprobar cuentas, firmar y seguir correspondencia; hacer y retirar giros y envíos; constituir, modificar, extinguir y liquidar contratos de todo tipo, particularmente de arrendamiento, aparcería, seguro, trabajo y transporte de cualquier clase, desahuciar inquilinos, arrendatarios, aparceros, colonos, porteros, precaristas y todo género de ocupantes; admitir y despedir obreros y empleados; reconocer, aceptar , pagar y cobrar cualesquiera deudas y créditos, por capital, intereses; dividendos y amortizaciones, y con relación a cualquiera persona o entidad pública o privada, incluso Estado, Provincia o Municipio, firmando recibos, saldos, conformidades y resguardos; asistir con voz y voto a juntas de regantes, propietarios, consocios, con dueños y demás cotitulares o de cualquier otra clase.
b) Disponer, enajenar, gravar, adquirir, vender y contratar, activa o pasivamente, respecto de toda clase de bienes muebles o inmuebles, derechos reales, y personales, acciones y obligaciones,

cupones, valores y cualesquiera efectos públicos o privados, pudiendo en tal sentido, con las condiciones y por el precio de contado, confesado o aplazado que estime pertinente, ejercitar, otorgar, conceder y aceptar compraventas, aportes, permutas, cesiones en pago y para pago, amortizaciones, rescates, subrogaciones, retractos, opciones y tanteos.

c) Comerciar, dirigir y administrar negocios mercantiles e industriales, realizando cualesquiera actos relativos al tráfico mercantil: tomar parte en concursos y subastas, formulando propuestas, reservas y protestas y aceptando adjudicaciones; constituir, modificar, prorrogar, disolver y liquidar toda clase de sociedades, ejercitar todos los derechos y obligaciones inherentes a la cualidad de socio y aceptar y desempeñar cargos en ellas.
d) Librar, aceptar, avalar, endosar, cobrar, pagar, intervenir y protestar letras de cambio, talones, cheques y otros efectos; abrir seguir, cancelar y liquidar libretas de ahorro, cuentas corrientes y de crédito, con garantía personal o de valores; concertar activa o pasivamente créditos comerciales; afianzar y dar garantías por otros; dar y tomar dinero en préstamo, con o sin interés, y con garantía personal, de valores o cualquier otra; constituir, transferir, modificar, cancelar y retirar depósitos provisionales o definitivos, de metálico, valores u otros bienes, comprar, vender canjear, pignorar y negociar efectos y valores, y cobrar sus intereses, dividendos y amortizaciones; arrendar cajas de seguridad, y, en general, operar con Cajas de Ahorros, Bancos, incluso el de España y otros oficiales, y entidades similares, disponiendo de los bienes existentes en ellos por cualquier concepto, y haciendo, en general, cuanto permitan la legislación y la práctica bancarias.
e) Comparecer en Juzgados, Tribunales, Magistraturas, Fiscalías, Sindicatos, Delegaciones, Jurados, Comisiones, Notarias, Registros y toda clase de oficinas públicas o privadas, autoridades y organismos del Estado, Provincias y Municipios, en asuntos civiles, penales, administrativos, contencioso y económico administrativos, gubernativos, laborales, fiscales y eclesiásticos, de todos los grados, jurisdicciones e instancias; promover, instar, seguir, contestar y terminar como actor, solicitante, coadyuvante, requerido/a, demandado/a, oponente o en cualquier otro concepto, toda clase de expedientes, actas, juicios, pretensiones, tramitaciones, excepciones, manifestaciones, reclamaciones, declaraciones, quejas y recursos, incluso de casación, con facultad de formalizar ratificaciones personales, desistimientos y allanamientos; otorgar, para los fines antedichos, poderes en favor de procuradores de los tribunales y abogados con las facultades usuales.

A efectos de la emisión de este tipo de certificados se darán por válidos los poderes que contengan un párrafo del siguiente tenor: “solicitar certificados electrónicos para la representación de la entidad para la realización de firma electrónica y la ejecución de transacciones electrónicas, contrataciones y cualquier otra actividad que requiera del uso de la firma electrónica o del certificado”.

4.1.12. Procedimiento simplificado de emisión de certificados

Se establecerá un procedimiento especial de registro simplificado para los casos en los que deba solicitarse un nuevo certificado por el cambio de alguno de los datos presentados por el Firmante respecto de una solicitud anterior.

El Firmante asumirá la responsabilidad mediante declaración firmada de la corrección de los datos no modificados.

La ER únicamente deberá comprobar la documentación que en su caso deba presentar el Firmante respecto de los datos cuya modificación ha declarado.

4.1.13. Requerimientos aplicables a las ER´s externas

Cuando la EC emplee ER’s externas deberá asegurar los siguientes aspectos:

- Que la identidad de la ER y de los administradores/operadores de la ER ha sido correctamente comprobada y validada.
- Que los administradores de la ER han recibido formación suficiente para el desempeño de sus funciones.
- Que la ER está autorizada para realizar las funciones de registro.
- Que la ER ha sido auditada por la EC, por una entidad externa o por el organismo de supervisión competente (INDECOPI).
- Que la ER asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones.
- Que la comunicación entre la ER y la EC, se realiza de forma segura mediante el uso de certificados digitales.

4.2. Re-emisión de la clave y del certificado

La re-emisión de un certificado es el proceso que debe realizarse para obtener un nuevo par de claves y un nuevo certificado cuando su fecha de expiración es cercana, el certificado haya expirado o haya sido revocado.

Un certificado podrá ser re-emitido solo bajo las siguientes circunstancias:

- Para Certificados de Persona Natural: la re-emisión sólo puede ser realizada una vez, para certificados cuya fecha de expiración es menor o igual a un año, antes de cumplirse el periodo de vigencia. El certificado re-emitido debe tener un periodo de vigencia máximo de un año.
- Para Certificados de Persona Jurídica - Atributos: la re-emisión sólo puede ser realizada una vez, para certificados cuya fecha de expiración es menor o igual a dos años. El certificado re-emitido debe tener un periodo de vigencia máximo de un año.
- Para Certificados de Sello electrónico de empresa para Agentes automatizados: la re-emisión sólo puede ser realizada una vez, cuando haya sido revocado un certificado digital antes de ser cumplido su periodo de vigencia.

En estos casos, la personación física del Solicitante puede no ser necesaria.

La EC deberá informar al Firmante antes de re-emitir, de los términos y condiciones que hayan cambiado respecto de la anterior emisión.

La EC en ningún caso emitirá un nuevo certificado usando la anterior clave pública del Firmante.

Actualmente, bajo la EC de Camerfirma Perú no se ejecutarán procesos de re-emisiones de certificados.

4.3. Modificación de certificados

Ante cualquier necesidad de modificación de certificados, la EC realizará una revocación del certificado y una nueva emisión con los datos corregidos.

4.4. Reemisión después de una revocación

La EC no realizará reemisiones después de una revocación de certificado.

4.5. Solicitud de revocación

Todas las solicitudes de revocación deberán ser autenticadas.

5. Requerimientos operacionales

5.1. Solicitud de certificados

La EC se asegurará de que los Firmantes están correctamente identificados y autorizados y que la petición del certificado es completa.

Registro

a) Antes de comenzar una relación contractual, la EC, por sí misma o por medio de la ER, deberá informar al solicitante de los términos y condiciones relativos al uso del certificado
b) Se deberá comunicar esta información a través de un medio de comunicación perdurable, susceptible de ser transmitido electrónicamente y en un lenguaje comprensible.
c) La EC, por sí misma o por medio de la ER, deberá comprobar, de acuerdo con la legislación vigente, la identidad y los atributos específicos del Firmante. La comprobación de la identidad del Firmante se realizará mediante los métodos indicados en el apartado 3.1.9 y la exhibición por éste de su documento de identidad (DNI, pasaporte, tarjeta de residencia o documento equivalente o mediante otro certificado según lo dispuesto en el apartado 3.1.9.)
d) Se registrará en todo caso:
    i. Nombre completo del Firmante.
    ii. Número del DNI, pasaporte o tarjeta de residencia del Firmante.
    iii. Nombre completo y forma jurídica de la Entidad (en caso de ser aplicable).
    iv. Evidencia de la existencia de la Entidad (en caso de ser aplicable).
    v. Evidencia de los poderes notariales del Firmante o de la vinculación con la Entidad (en caso de ser aplicable).
e) El solicitante deberá facilitar su dirección física u otros datos que permitan contactar con él.
f) La EC deberá registrar toda la información usada para comprobar la identidad de los Firmantes/Suscriptores, incluyendo cualquier número de referencia en la documentación empleada para la verificación y los límites de su validez. En particular, se recomienda el uso de los servicios web del Registro Nacional de Identificación y estado Civil (RENIEC).
g) La EC deberá guardar el contrato firmado con el Firmante, el cual incluirá:
    i. Acuerdo de las obligaciones del Firmante.
    ii. Compromiso del Firmante a usar el dispositivo de creación de firma ofrecido por la EC de forma diligente.
    iii. Consentimiento para que la EC guarde la información usada para el registro, entrega del dispositivo del Firmante, para una futura revocación, así como para el traspaso de información a una tercera parte en el caso de que la EC cese su actividad.
    iv. Si y bajo qué condiciones el Firmante consiente la publicación del certificado.
    v. Que la información contenida en el certificado es correcta
h) Los registros identificados deberán conservarse durante el periodo de tiempo que se indicó al Firmante en el contrato y que es necesario a efectos probatorios en los procedimientos legales (mínimo 10 años). En particular, se recomienda el uso de armario corta fuego para la custodia de la documentación entregada por el Solicitante. Alternativamente a la conservación de los expedientes en archivos físicos, la EC o la ER podrán utilizar los servicios de digitalización y

custodia documental con valor legal a través de digitalización y microformas conforme lo permite la norma vigente, con copia de seguridad. Asimismo, se podrá eliminar los archivos físicos, utilizando dichos sistemas de digitalización y archivo electrónico, haciendo constar por fedatario informático el traspaso de lo físico a lo digital.

i) Si el par de claves no es generado por la EC, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el Firmante está en posesión de la clave privada asociada a la clave pública.

j) La EC deberá cumplir con todos los requisitos impuestos por la legislación aplicable en materia de protección de datos.

5.2. Petición de certificación cruzada

La EC identificará los procesos necesarios para realizar certificación cruzada.

La EC deberá revisar cualquier petición de certificación cruzada y aprobar o denegar dicha petición.

Una petición de certificación cruzada deberá incluir en todo caso su política de certificación, un informe de auditoría externa aprobando el nivel de seguridad establecido en la política de certificación y la clave pública de verificación de la EC.

5.3. Emisión de certificados

La EC deberá poner todos los medios a su alcance para asegurar que la emisión y en su caso, la re-emisión de certificados se realiza de una forma segura. En particular:

- Cuando la EC genere las claves del Firmante, que el procedimiento de emisión del certificado está ligado de manera segura a la generación del par de claves por la EC
- Cuando la EC no genere las claves del Firmante, que la clave privada o el dispositivo seguro de creación de firma ha sido generado de manera segura por el Firmante.
- La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los DN asignados a los Firmantes.
- La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados con el Firmante o entre distintos componentes del sistema de certificación.
- La EC deberá verificar que el registro de los datos es intercambiado con proveedores de servicios reconocidos, cuya identidad es autenticada.
- La EC deberá notificar al solicitante la emisión de su certificado.

5.4. Aceptación de certificados

La entrega del certificado y la firma de las condiciones de utilización del sistema de certificación implicará la aceptación del certificado por parte del Firmante.

La aceptación del certificado deberá realizarse de forma expresa, por escrito y ante el encargado de la EC o ER. El solicitante emitirá esta aceptación en su propio nombre.

No obstante, a partir de la entrega del certificado, existirá un periodo de catorce días naturales para revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad. En caso de que existiera alguna diferencia entre los datos suministrados a la EC y el contenido del certificado, ello

deberá ser comunicado de inmediato a la EC para que proceda a su revocación y a la emisión de un nuevo certificado. La EC entregará el nuevo certificado sin coste para el Firmante en el caso de que la diferencia entre los datos sea causada por un error no imputable al Firmante. Transcurrido dicho periodo sin que haya existido comunicación se entenderá que el Firmante ha confirmado la aceptación del certificado y de todo su contenido.

Aceptando el certificado, se confirma y asume la exactitud del contenido de este, con las consiguientes obligaciones que de ello se deriven frente a la ER, la EC o cualquier tercero que de buena fe confíe en el contenido del Certificado.

5.5. Suspensión y revocación de certificados

5.5.1. Aclaraciones previas

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de un certificado en función de alguna circunstancia distinta a la caducidad de este. Al hablar de revocación nos referiremos siempre a la pérdida de validez definitiva.

La suspensión por su parte supone una revocación con causa de suspensión, esto es, se revoca un certificado temporalmente hasta que se decida sobre la oportunidad o no de realizar una revocación definitiva.

Por tanto, a efectos de la presente política de certificación, hablaremos de revocación para referirnos a aquella revocación de carácter definitivo y a la suspensión como aquella revocación con causa de suspensión.

5.5.2. Causas de revocación

Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Firmante.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del Firmante o incapacidad sobrevenida, total o parcial.
- Terminación de la vinculación del Firmante con la Entidad o pérdida de los poderes de representación.
- Cese en la actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el solicitante para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Que se detecte que las claves privadas del Firmante o de la EC han sido comprometidas, bien porque concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualesquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
- Por incumplimiento por parte de la ER, EC o el Firmante de las obligaciones establecidas en esta política.
- Por la resolución del contrato con el Firmante.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la extinción de la Entidad.

- Por la concurrencia de cualquier otra causa especificada en la presente política.

5.5.3. Quien puede solicitar la revocación

La revocación de un certificado podrá solicitarse únicamente por el Firmante, la Entidad a través de su representante legal o por la propia EC.

Todas las solicitudes de revocación deberán ser en todo caso autenticadas.

5.5.4. Procedimiento de solicitud de revocación

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son revocados basándose en peticiones de revocación autorizadas y validadas.

La información relativa al retraso máximo entre la recepción de una petición de revocación y su paso al estado de suspendido estará disponible para todas las Partes Usuarias. Este deberá ser como máximo de 3 horas.

Un certificado permanecerá suspendido mientras la revocación no sea confirmada. La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que un certificado no permanece en estado suspendido por más tiempo que el necesario para confirmar la procedencia o no de la revocación.

El Firmante cuyo certificado haya sido suspendido o revocado deberá ser informado del cambio de estado del certificado. Así mismo, el Firmante deberá ser informado del levantamiento de la suspensión.

La EC utilizará todos los medios a su alcance para conseguir este objetivo, pudiendo intentar la mencionada comunicación por e-mail, teléfono, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

Una vez que un certificado es revocado (no suspendido), este no podrá volver a su estado activo. La revocación de un certificado es una acción, por tanto, definitiva.

Cuando se usen listas de certificados revocados (CRLs) que incluyan algunas variantes (p. Ej. Delta CRLs), estas serán publicadas al menos semanalmente.

La CRL, en su caso, será firmada por la EC o por una autoridad de confianza de la EC.

El servicio de gestión de las revocaciones estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la EC, la EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

La información relativa al estado de la revocación estará disponible las 24 del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la EC, la EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

Se deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la autenticidad y la confidencialidad de la información relativa al estado de los certificados.

La información relativa al estado de los certificados deberá estar disponible públicamente.

5.5.5. Periodo de revocación

La decisión de revocar o no un certificado no podrá retrasarse por un periodo máximo de 2 semanas.

5.5.6. Suspensión

La suspensión, a diferencia de la revocación supone la pérdida de validez temporal de un certificado.

5.5.7. Procedimiento para la solicitud de suspensión

La solicitud de suspensión se realizará a través de una llamada telefónica al servicio de gestión de las revocaciones o por medio de un servicio on-line de suspensiones en la página web de la EC.

5.5.8. Límites del periodo de suspensión

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que un certificado no permanece suspendido por más tiempo que el necesario para confirmar la procedencia o no de la revocación.

5.5.9. Frecuencia de emisión de CRL

La EC proporcionará la información relativa a la revocación de los certificados a través de una CRL.

La EC actualizará y publicará la CRL dentro de las 3 horas siguientes a la recepción de una solicitud de suspensión que haya sido previamente validada, y al menos con una frecuencia semanal si no se han producido cambios en la CRL.

5.5.10. Requisitos de comprobación de CRL

Las Partes Usuarias podrán comprobar el estado de los certificados en los cuales va a confiar, debiendo comprobar en todo caso la última CRL emitida. No obstante, la AC podrá imponer una tarifa por el acceso a la CRL.

5.5.11. Disponibilidad de comprobación on-line de la revocación

Se proporcionará un servicio on-line de comprobación de revocaciones, el cual estará disponible las 24 horas del día los 7 días de la semana. En caso de fallo del sistema, del servicio o de cualquier otro factor que no esté bajo el control de la EC, la EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

5.5.12. Requisitos de la comprobación on-line de la revocación

La Parte Usuaria que desee comprobar la revocación de un certificado, podrá hacerlo de forma on-line a través de la página web de la EC www.camerfirma.com

La EC dispondrá de un sistema de consulta que impida la obtención masiva de datos relativos a los Firmantes, por lo que para la obtención del estado de un certificado deberán conocerse algunos parámetros del mismo como el e-mail.

No obstante lo anterior, el acceso a este sistema de consulta de certificados será libre y gratuito.

5.5.13. Otras formas de divulgación de información de revocación disponibles

No estipulado.

5.5.14. Requisitos de comprobación para otras formas de divulgación de información de revocación

No estipulado.

5.5.15. Requisitos especiales de revocación por compromiso de las claves

No estipulado.

5.6. Procedimientos de control de seguridad

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relevante concerniente a un certificado es conservada durante el periodo de tiempo que pueda ser necesario a efectos probatorios en los procedimientos legales y al menos durante 10 años. En particular:

General

a) Se deberán realizar los esfuerzos que razonablemente estén a su alcance para confirmar la confidencialidad y la integridad de los registros relativos a los certificados, tanto de los actuales como de aquellos que hayan sido previamente almacenados.
b) Los registros relativos a los certificados deberán ser almacenados completa y confidencialmente de acuerdo con las prácticas de negocio.
c) Los registros relativos a los certificados deberán estar disponibles si estos son requeridos a efectos probatorios en los procedimientos legales
d) El momento exacto en que se produjeron los eventos relativos a la gestión de las claves y la gestión de los certificados deberá ser almacenado.
e) Los registros relativos a los certificados serán mantenidos durante un periodo de tiempo necesario para dotar de la evidencia legal necesaria a las firmas electrónicas.
f) Los eventos se registrarán de manera que no puedan ser fácilmente borrados o destruidos (excepto para su transferencia a medios duraderos) durante el periodo de tiempo en el que deban ser conservados.
g) Los eventos específicos y la fecha de registro serán documentados por la EC.

Registro

h) La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que todos los eventos relativos al registro, incluyendo las peticiones de re-emisión en su caso y revocación serán registrados.
i) La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relativa al registro es almacenada, incluyendo la siguiente:
    i. La documentación presentada por el solicitante para el registro.
    ii. Número de DNI, pasaporte o de cualquier otro documento acreditativo de la identidad del solicitante.
    iii. Copia de documentos identificativos (DNI, pasaporte,...), incluido el contrato suscrito con el Firmante.

iv. Algunas cláusulas específicas contenidas en el contrato (p.ej. el consentimiento de la publicación del certificado).
v. Método empleado para comprobar la validez de los documentos identificativos, si existe.
vi. Nombre de la Entidad de Registro.

j) La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la privacidad de la información relativa al Firmante.

Generación del certificado

k) La EC registrará todos los eventos relativos al ciclo de vida de las claves de la AC.
l) La EC registrará todos los eventos relativos al ciclo de vida de los certificados.

Entrega del dispositivo al Firmante

m) La EC registrará todos los eventos relativos al ciclo de vida de las claves gestionadas por la misma, incluyendo las claves de los Firmantes/Suscriptores generadas por la EC.

Gestión de la revocación

n) La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las peticiones e informes relativos a una revocación, así como su resultado, son registrados.

5.6.1. Tipos de eventos registrados

Toda la información auditada y especificada en el apartado anterior deberá ser archivada.

La EC registrará y guardará los logs de todos los eventos relativos al sistema de seguridad de la EC.

Estos incluirán eventos como:

- encendido y apagado del sistema.
- encendido y apagado de la aplicación de la EC.
- intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- cambios en los detalles de la EC y/o sus claves.
- cambios en la creación de políticas de certificados.
- intentos de inicio y fin de sesión.
- intentos de accesos no autorizados al sistema de la EC a través de la red.
- intentos de accesos no autorizados al sistema de archivos.
- generación de claves propias.
- creación y revocación de certificados.
- intentos de dar de alta, eliminar, habilitar y deshabilitar Firmantes/Suscriptores y actualizar.
- acceso físico a los logs.
- cambios en la configuración y mantenimiento del sistema.
- cambios personales.
- registros de la destrucción de los medios que contienen las claves, datos de activación.

5.6.2. Frecuencia de procesado de logs

La EC deberá revisar sus logs periódicamente y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente.

La EC deberá así mismo asegurarse de que los logs no han sido manipulados y deberán documentar las acciones tomadas ante esta revisión

5.6.3. Periodos de retención para los logs de auditoría

La información almacenada deberá ser conservada al menos durante 10 años.

5.6.4. Protección de los logs de auditoría

El soporte de almacenamiento de los logs debe ser protegido por seguridad física, o por una combinación de seguridad física y protección criptográfica. Además, será adecuadamente protegido de amenazas físicas como la temperatura, la humedad, el fuego y la magnetización.

5.6.5. Procedimientos de backup de los logs de auditoría

Debe establecerse un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

5.6.6. Sistema de recogida de información de auditoría

No estipulado.

5.6.7. Notificación al sujeto causa del evento

No estipulado.

5.6.8. Análisis de vulnerabilidades

Se deberá realizar una revisión de riesgos de seguridad para la totalidad del sistema. Esta revisión cubrirá la totalidad de riesgos que pueden afectar a la emisión de certificados y se realizará con una periodicidad trimestral.

5.7. Archivo de registros

5.7.1. Tipo de archivos registrados

Los siguientes datos y archivos deben ser almacenados por la EC o por delegación de esta.

- todos los datos de la auditoría.
- todos los datos relativos a los certificados, incluyendo los contratos con los Firmantes/Suscriptores y los datos relativos a su identificación.
- solicitudes de emisión y revocación de certificados.
- todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- la documentación requerida por los auditores.
- historial de claves generadas.
- las comunicaciones entre los elementos de la PKI.

La EC es responsable del correcto archivo de todo este material.

5.7.2. Periodo de retención para el archivo

La información detallada en el apartado 4.6 h), k) y l), los contratos con los Firmantes y cualquier información relativa a la identificación y autenticación del Firmante deberá ser conservada durante al menos 10 años desde la extinción o revocación del certificado. La destrucción de un archivo de auditoría correspondiente a un servicio brindado en el Estado Peruano sólo se podrá llevar a cabo con la autorización de INDECOPI.

5.7.3. Protección del archivo

El soporte de almacenamiento debe ser protegido por medio de seguridad física, o por una combinación de seguridad física y protección criptográfica. Además, el soporte será adecuadamente protegido amenazas físicas como la temperatura, la humedad, el fuego y la magnetización.

5.7.4. Procedimientos de backup del archivo

Debe establecerse un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes estén disponibles en un periodo corto de tiempo las correspondientes copias de backup.

5.7.5. Requerimientos para el sellado de tiempo de los registros

No estipulado.

5.7.6. Sistema de recogida de información de auditoría

No estipulado.

5.7.7. Procedimientos para obtener y verificar información archivada

La AC dispondrá de un procedimiento adecuado que limite la obtención de información sólo a las personas debidamente autorizada.

Este procedimiento deberá regular tanto los accesos a la información internos como externos, debiendo exigir en todo caso un acuerdo de confidencialidad previo a la obtención de la información.

5.8. Cambio de clave de la EC

Antes de que el uso de la clave privada de la EC caduque se deberá realizar un cambio de claves. La vieja EC y su clave privada se desactivarán y se generara una nueva AC con una clave privada nueva y un nuevo DN.

5.9. Recuperación en caso de compromiso de la clave o desastre

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar en caso de desastre o compromiso de la clave privada de la AC que éstas serán restablecidas tan pronto como sea posible. En particular:

5.9.1. La clave de la EC se compromete

El plan de la continuidad de negocio de la EC (o el plan de contingencia) tratará el compromiso o el compromiso sospechado de la clave privada de la EC como un desastre.

En caso de compromiso, la EC tomará como mínimo las siguientes medidas:

- Informar a todos los Firmantes, Partes Usuarias y otras ECs con los cuales tenga acuerdos u otro tipo de relación del compromiso.
- Indicar que los certificados e información relativa al estado de la revocación firmados usando esta clave pueden no ser válidos.
- Suspender la emisión de certificados durante el tiempo que persista dicho incidente.

5.9.2. Instalación de seguridad después de un desastre natural u otro tipo de desastre

La EC debe tener un plan apropiado de contingencias para la recuperación en caso de desastres.

La EC debe reestablecer los servicios de acuerdo con esta política dentro de las 24 horas posteriores a un desastre o emergencia imprevista. Tal plan incluirá una prueba completa y periódica de la preparación para tal restablecimiento.

5.10. Cese de la EC

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se minimizan los posibles perjuicios que se puedan crear a los Firmantes o Partes Usuarias como consecuencia del cese de su actividad y en particular del mantenimiento de los registros necesarios a efectos probatorios en los procedimientos legales. En particular:

a) Antes del cese de su actividad deberá realizar, como mínimo, las siguientes actuaciones:
   i. Informar a todos los Firmantes, Partes Usuarias, Autoridades Administrativas Competentes (AAC) que supervisan la actividad de Camerfirma y Camerfirma Perú, así como en su caso, y las otras ECs con los cuales tenga acuerdos u otro tipo de relación del cese.
   ii. Publicará en su página web o cualquier otro medio accesible para los usuarios, la información pertinente concerniente a la conclusión de sus operaciones.
   iii. La EC revocará toda autorización a entidades subcontratadas para actuar en nombre de la EC en el procedimiento de emisión de certificados.
   iv. Transferirá a otro Prestador o a la Autoridad Administrativa Competente, los datos necesarios para la continuidad de las operaciones bajo el marco legal aplicable, en particular los certificados raíz, listas de certificados revocados y sus obligaciones relativas al mantenimiento de la información del registro, archivos de log de eventos y de los registros de auditoría durante el periodo de tiempo indicado a los Firmantes y usuarios en el contrato de suscripción.
   v. Las claves privadas de la EC serán destruidas deshabilitadas para su uso.
b) La EC tendrá contratado un seguro que cubra hasta el límite contratado los costes necesarios para satisfacer estos requisitos mínimos en caso de quiebra o por cualquier otro motivo por el que no pueda hacer frente a estos costes por sí mismo.
c) Se establecerán en la DPC las previsiones hechas para el caso de cese de actividad. Estas incluirán:
   i. informar a las entidades afectadas.
   ii. transferencia de las obligaciones de la EC a otras partes.
   iii. cómo debe ser tratada la revocación de certificados emitidos cuyo periodo de validez aún no ha expirado.

En particular, la EC deberá:

i. informar puntualmente a todos los Firmantes, empleados, Partes Usuarias y ERs con una anticipación mínima de 6 meses antes del cese.
ii. transferir todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación.

6. Controles de seguridad física, procedimental y de personal

6.1. Controles de seguridad física

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso físico a los servicios críticos y que los riesgos físicos de estos elementos sean minimizados. En particular:

EC General

a) El acceso físico a las instalaciones vinculadas a la generación de certificados, entrega del dispositivo al Firmante y servicios de gestión de revocaciones deberá ser limitado a las personas autorizadas y las instalaciones en las que se firman los certificados deberán ser protegidas de las amenazas físicas.
b) Se establecerán controles para impedir la perdida, daño o compromiso de los activos de la empresa y la interrupción de la actividad.
c) Se establecerán controles para evitar el compromiso o robo de información.

Generación de certificados, entrega del dispositivo del Firmante y gestión de revocaciones.

d) Las actividades relativas a la generación de certificados y gestión de revocaciones serán realizadas en un espacio protegido físicamente de accesos no autorizados al sistema o a los datos.
e) La protección física se conseguirá por medio de la creación de unos anillos de seguridad claramente definidos (p.ej. barreras físicas) alrededor de la generación de certificados y gestión de revocaciones. Aquellas partes de esta tarea compartidas con otras organizaciones quedarán fuera de este perímetro.
f) Los controles de seguridad física y medioambiental serán implementados para proteger las instalaciones que albergan los recursos del sistema, los recursos del sistema en sí mismos y las instalaciones usadas para soportar sus operaciones. Los programas de seguridad física y medioambiental de la AC relativos a la generación de certificados, entrega del dispositivo del Firmante y servicios de gestión de revocaciones estarán provistos de controles de acceso físico, protección ante desastres naturales, sistemas anti-incendios, fallos eléctricos y de telecomunicaciones, humedad, protección antirrobo,...
g) Se implementarán controles para evitar que los equipos, la información, soportes y software relativos a los servicios de la AC sean sacados de las instalaciones sin autorización.

6.1.1. Ubicación y construcción

Las instalaciones de la EC deben ubicadas en una zona de bajo riesgo de desastres y que permita un rápido acceso a las mismas conforme al plan de contingencias.

Así mismo, las instalaciones estarán equipadas con los elementos y materiales adecuados para poder albergar información de alto valor.

6.1.2. Acceso físico

El acceso físico a las zonas de seguridad estará limitado al personal autorizado previa autenticación.

6.1.3. Alimentación eléctrica y aire acondicionado

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la alimentación eléctrica y el aire acondicionado son suficientes para soportar las actividades del sistema de la EC.

6.1.4. Exposición al agua

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de EC está protegido de la exposición al agua.

6.1.5. Protección y prevención de incendios

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de EC está protegido con un sistema antincendios.

6.1.6. Sistema de almacenamiento

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de almacenamiento usado por el sistema de EC está protegido de riesgos medioambientales como la temperatura, la humedad y la magnetización.

6.1.7. Eliminación de residuos

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los medios usados para almacenar o transmitir la información de carácter sensible como las claves, datos de activación o archivos de la EC serán destruidos, así como que la información que contengan será irrecuperable.

6.1.8. Backup remoto

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las instalaciones usadas para realizar back-up externo, que tendrán el mismo nivel de seguridad que las instalaciones principales.

6.2. Controles procedimentales

6.2.1. Roles de confianza

Los roles de confianza, en los cuales se sustenta la seguridad de la EC, serán claramente identificados.

Los roles de confianza incluyen las siguientes responsabilidades:

- **Responsable de seguridad**: asume la responsabilidad por la implementación de las políticas de seguridad, así como gestión y revisión de logs.

- **Administradores de sistema**: Están autorizados para instalar, configurar y mantener los sistemas y aplicaciones de confianza de la AC que soportan las operaciones de Certificación.
- **Operador de sistema**: Está autorizado para realizar funciones relacionadas con el sistema de backup y de recuperación.
- **Administrador de CA**: Responsable de la Administración y control de gestión de los sistemas de confianza de la EC.
- **Operador de CA**: Realizan funciones de apoyo en el control dual de las operaciones de la EC.
- **Auditor de CA**: Realiza las labores de supervisión y control de la implementación de las políticas de seguridad.

La EC debe asegurarse que existe una separación de tareas para las funciones críticas de la EC para prevenir que una persona use el sistema el sistema de EC y la clave de la EC sin detección.

La separación de los roles de confianza será detallada en la DPC.

6.2.2. Número de personas requeridas por tarea

Las siguientes tareas requerirán al menos un control dual:

- La generación de la clave de la EC.
- La recuperación y back-up de la clave privada de la EC.
- Activación de la clave privada de la EC.
- Cualquier actividad realizada sobre los recursos HW y SW que dan soporte a la autoridad de certificación.

6.2.3. Identificación y autenticación para cada rol

La EC establecerá los procedimientos de identificación y autenticación de las personas implicadas en roles de confianza.

6.3. Controles de seguridad de personal

6.3.1. Requerimientos de antecedentes, calificación, experiencia y acreditación

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal cumple con los requisitos mínimos razonables para el desempeño de sus funciones. En concreto:

EC General

a) La EC empleará personal que posea el conocimiento, experiencia y calificaciones necesarias y apropiadas para el puesto.
b) Los roles de seguridad y responsabilidades especificadas en la política de seguridad de la EC, serán documentadas en la descripción del trabajo.
c) Se deberá describir el trabajo del personal de la EC (temporal y fijo) desde el punto de vista de realizar una separación de tareas, definiendo los privilegios con los que cuentan, los niveles de acceso y una diferenciación entre las funciones generales y las funciones específicas de la EC.
d) El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.

Registro, generación de certificados y gestión de revocaciones

e) Deberá ser empleado el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de firma electrónica y esté familiarizado con procedimientos de seguridad.
f) Todo el personal implicado en roles de confianza deberá estar libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de la EC.
g) El personal de la EC será formalmente designado para desempeñar roles de confianza por el responsable de seguridad.
h) La EC no asignará funciones de gestión a una persona cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

6.3.2. Procedimientos de comprobación de antecedentes

La EC no podrá asignar funciones que impliquen el manejo de elementos críticos del sistema a aquellas personas que no posean la experiencia necesaria en la propia EC que propicie la confianza suficiente en el empleado. Se entenderá como experiencia necesaria el haber pertenecido al Departamento en cuestión durante al menos 6 meses.

6.3.3. Requerimientos de formación

La AC debe realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal que realiza tareas de operaciones de EC o ER, recibirá una formación relativa a:

- los principales mecanismos de seguridad de EC y/o ER.
- todo el software de PKI y sus versiones empleados en el sistema de la EC.
- todas las tareas de PKI que se espera que realicen.
- los procedimientos de resolución de contingencias y continuidad de negocio.

6.3.4. Requerimientos y frecuencia de la actualización de la formación

La formación debe darse con una frecuencia anual para asegurar que el personal está desarrollando sus funciones correctamente.

6.3.5. Frecuencia y secuencia de rotación de tareas

No estipulado.

6.3.6. Sanciones por acciones no autorizadas

La EC deberá fijar las posibles sanciones por la realización de acciones no autorizadas.

6.3.7. Requerimientos de contratación de personal

Ver el apartado 5.3.1 de este documento.

6.3.8. Documentación proporcionada al personal

Todo el personal de la EC y ER deberá recibir los manuales de Partes Usuarias en los que se detallen al menos los procedimientos para el registro de certificados, creación, actualización, re-emision si aplica, suspensión, revocación y la funcionalidad del software empleado.

7. Controles de seguridad técnica

7.1. Generación e instalación del par de claves

7.1.1. Generación del par de claves de la EC

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de la EC sean generadas de acuerdo a los estándares.

En particular:

a) La generación de la clave de la EC se realizará en un entorno seguro físicamente por el personal adecuado según los roles de confianza y, al menos con un control dual. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la DPC.
b) La generación de la clave de la EC se realizará en un dispositivo que cumpla los requerimientos que se detallan en el FIPS 140-2, en su nivel 3 o superior.

7.1.2. Generación del par de claves del firmante

El par de claves será generado por el emisor o bajo su control.

Si las claves del Firmante son generadas por la EC, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves son generadas de forma segura y que se mantendrá la privacidad de las mismas. En particular:

a) Las claves serán generadas usando un algoritmo adecuado para los propósitos de la firma electrónica avanzada.
b) Las claves tendrán una longitud de clave adecuada para los propósitos de la firma electrónica avanzada y para el algoritmo de clave pública empleado.
c) Las claves serán generadas y guardadas de forma segura antes de entregárselas al responsable de la entidad.
d) Las claves serán destruidas de forma segura después de su entrega al responsable de la entidad.

7.1.3. Entrega de la clave privada al firmante

Cuando la clave privada del Firmante sea generada por la EC, ésta le será entregada de manera que la confidencialidad de la misma no sea comprometida y sólo el Firmante tenga acceso a la misma.

La clave privada deberá ser almacenada en todo caso en un dispositivo seguro de almacenamiento de los datos de creación de firma (DSADCF) o en dispositivo seguro de creación de firma (DSCF).

Así mismo, este dispositivo seguro podrá consistir en un medio de almacenamiento externo (p. ej smartcard o key token), en un medio software (p. ej. PKCS#12) o en formato firma remota (nube).

Cuando la EC entrega un dispositivo seguro al responsable de la entidad, deberá hacerlo de forma segura. En particular:

a) La preparación del dispositivo seguro, deberá ser controlada de manera segura por el proveedor de servicios.
b) El dispositivo seguro será guardado y distribuido de forma segura.

c) Cuando el dispositivo seguro tenga asociado unos datos de activación de Parte Usuaria que confía (p.ej. un código PIN), los datos de activación se deberán preparar de forma segura y distribuirse de manera separada del dispositivo seguro de creación de firma

7.1.4. Entrega de la clave pública del firmante al emisor del certificado

Cuando el Firmante pueda generar sus propias claves, la clave pública del Firmante tiene que ser transferida a la ER o EC, de forma que se asegure que,

- no ha sido cambiado durante el traslado.
- el remitente está en posesión de la clave privada que se corresponde con la clave pública transferida y
- el proveedor de la clave pública es la legítima Parte Usuaria que confía que aparece en el certificado

7.1.5. Entrega de la clave pública de la EC a las partes usuarias

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la integridad y la autenticidad de la clave pública de la AC y los parámetros a ella asociados son mantenidos durante su distribución a las Partes Usuarias. En particular:

a) La clave pública de la EC estará disponible a las Partes Usuarias de manera que se asegure la integridad de la clave y se autentique su origen.
b) El certificado de la EC y su fingerprint (huella digital) estarán a disposición de las Partes Usuarias a través de su página Web.

7.1.6. Tamaño y periodo de validez de las claves del emisor

El emisor deberá usar claves basadas en el algoritmo **RSA** con una longitud mínima de **4.096 bits** para firmar certificados.

El periodo de uso de una clave privada será como máximo de **24 años**, después del cual deberán cambiarse estas claves.

El periodo de validez del certificado de la EC se establecerá como mínimo en atención a lo siguiente:

- El periodo de uso de la clave privada de la EC, y
- El periodo máximo de validez de los certificados de los Firmantes/Suscriptores firmados con esa clave.

7.1.7. Tamaño y periodo de validez de las claves del firmante

El Firmante deberá usar claves basadas en el algoritmo **RSA** con una longitud mínima de **2.048 bits**.

El periodo de uso de la clave pública y privada del Firmante no deberá ser superior a **4 años** y no excederá del periodo durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

7.1.8. Parámetros de generación de la clave pública

No estipulado.

7.1.9. Comprobación de la calidad de los parámetros

No estipulado.

7.1.10. Hardware/Software de generación de claves

El par de claves de los Suscriptores serán generadas por el prestador o EC.

7.1.11. Fines del uso de la clave

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de firma de la EC son usadas sólo para los propósitos de generación de certificados y para la firma de CRLs.

La clave privada del Firmante deberá ser usada únicamente para la generación de firmas electrónicas avanzadas.

7.2. Protección de la clave privada

De la EC

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves privadas de la EC continúan siendo confidenciales y mantienen su integridad. En particular:

- La clave privada de firma de la EC será mantenida y usada en un dispositivo criptográfico seguro, el cual cumple los requerimientos que se detallan en el FIPS 140-2, en su nivel 3 o superior.
- Cuando la clave privada de la EC esté fuera del módulo criptográfico esta deberá estar cifrada.
- Se deberá hacer un back up de la clave privada de firma de la EA, que deberá ser almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la DPC.
- Las copias de back up de la clave privada de firma de la EC se regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

Del Firmante

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada está protegida de forma que:

- el Firmante o un responsable suyo pueda mantener la clave privada bajo su exclusivo control,
- su secreto está razonablemente asegurado, y
- la clave privada puede ser efectivamente protegida por el Firmante o un responsable suyo contra un uso ajeno

7.3. Estándares para los módulos criptográficos

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 3 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente.

7.3.1. Control multipersona (n de entre m) de la clave privada

Se requerirá un control multipersona para la activación de la clave privada de la EC. Este control deberá ser definido adecuadamente por la DPC en la medida en que no se trate de información confidencial o pueda comprometer de algún modo la seguridad del sistema.

7.3.2. Depósito de la clave privada (key escrow)

No estipulado.

7.3.3. Copia de seguridad de la clave privada

La EC deberá realizar una copia de back up de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de la misma de acuerdo con el apartado anterior.

Las copias de las claves privadas de los Firmantes se regirán por lo dispuesto en el punto anterior.

7.3.4. Archivo de la clave privada

La clave privada de la EC no podrá ser archivada una vez finalizado su ciclo de vida.

Las claves privadas de Firmante no pueden ser archivadas por la EC, salvo que legalmente se prevea la posibilidad de dicho almacenamiento.

7.3.5. Introducción de la clave privada en el módulo criptográfico

Ya visto.

7.3.6. Método de activación de la clave privada

La clave privada de la EC deberá ser activada conforme al apartado 6.3.1.

Se deberá proteger el acceso a la clave privada del Firmante por medio de un password, PIN, u otros métodos de activación equivalentes. Si estos datos de activación deben ser entregados al Firmante, esta entrega deberá realizarse por medio de un canal seguro.

Estos datos de activación deberán tener una longitud de al menos 4 dígitos en el caso de custodia en un dispositivo hardware y de 8 en el caso de dispositivo software.

Los datos de activación deben ser memorizados por el Firmante y no deben ser anotados en un lugar de fácil acceso ni compartidos.

7.3.7. Método de desactivación de la clave privada

La clave privada del Firmante podrá quedar inaccesible después de sucesivos intentos en la introducción del código de activación.

7.3.8. Método de destrucción de la clave privada

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada de la EC no será usada una vez finalizado su ciclo de vida.

Todas las copias de la clave privada de firma de la EC deberán ser destruidas o deshabilitadas de forma que la clave privada no pueda ser recuperada.

La destrucción o des-habilitación de las claves se detallará en un documento creado al efecto.
Las claves privadas de los Firmantes deberán ser destruidas o hacerlas inservibles después del fin de su ciclo de vida por el propio Firmante.

7.4. Otros aspectos de la gestión del par de claves

7.4.1. Archivo de la clave pública

La EC deberá conservar todas las claves públicas de verificación.

7.4.2. Periodo de uso para las claves públicas y privadas

Ya visto.

7.5. Datos de activación

7.5.1. Generación y activación de los datos de activación

Los datos de activación de las EC se generan y se almacenan en smart cards criptográficas únicamente en posesión de personal autorizado.

7.5.2. Protección de los datos de activación

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación.

7.5.3. Otros aspectos de los datos de activación

No estipulado.

7.6. Ciclo de vida del dispositivo seguro de almacenamiento de los datos de creación de firma (DSADCF) y del dispositivo seguro de creación de firma (DSCF)

La EC deberá, por si misma o por delegación de esta función, realizar los mayores para asegurar que:

a) La preparación del DSADCF o DSCF es controlada de forma segura.
b) El DSADCF o DSCF es almacenado y distribuido de forma segura.
c) Si el propio sistema lo permite, que la activación y desactivación del DSADCF o DSCF es controlada de forma segura.
d) El DSADCF o DSCF no es usado por la EC o entidad delegada antes de su emisión.
e) El DSADCF o DSCF queda inhabilitado para su uso en caso de ser devuelto por el Firmante.
f) Cuando el DSADCF o DSCF lleve asociado unos datos de activación (ej PIN), estos datos de activación y el dispositivo seguro de creación de firma serán preparados y distribuidos de forma separada.

7.7. Controles de seguridad informática

La EC empleará sistemas fiables y productos que estén protegidos contra modificaciones. En particular, los sistemas deberán cumplir las siguientes funciones:

- identificación de todos las Partes Usuarias.
- controles de acceso basados en privilegios.
- control dual para ciertas operaciones relativas a la seguridad.
- generación de logs, revisión de auditoría y archivo de todos los eventos relacionados con la seguridad.
- backup y recuperación.

7.7.1. Requerimientos técnicos de seguridad informática específicos

Cada servidor de EC incluirá las siguientes funcionalidades:

- control de acceso a los servicios de EC y gestión de privilegios.
- imposición de separación de tareas para la gestión de privilegios.
- identificación y autenticación de roles asociados a identidades.
- archivo del historial del Firmante y la EC y datos de auditoría.
- auditoría de eventos relativos a la seguridad.
- auto-diagnóstico de seguridad relacionado con los servicios de la EC.
- Mecanismos de recuperación de claves y del sistema de EC.

Las funcionalidades de arriba pueden ser provistas por el sistema operativo o mediante una combinación de sistemas operativos, software de PKI y protección física.

7.7.2. Valoración de la seguridad informática

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

7.8. Controles de seguridad del ciclo de vida

7.8.1. Controles de desarrollo del sistema

La EC empleará sistemas fiables y productos con un nivel de seguridad suficiente para la funcionalidad y seguridad que se exige.

7.8.2. Controles de gestión de la seguridad

Gestión de seguridad

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los procedimientos administrativos y de gestión son aplicados, son adecuados y se corresponden con los estándares reconocidos. En particular:

a) La EC será responsable por todos los aspectos relativos a la prestación de servicios de certificación, incluso si algunas de sus funciones han sido subcontratadas con terceras partes. Las responsabilidades de las terceras partes serán claramente definidas por la EC en los acuerdos concretos que la EC suscriba con esas terceras partes para asegurar que éstas están

obligadas a implementar cualquier control requerido por la EC. La EC será responsable por la revelación de prácticas relevantes.

b) La EC deberá desarrollar las actividades necesarias para la formación y concienciación de los empleados en material de seguridad.
c) La información necesaria para gestionar la seguridad de la EC deberá mantenerse en todo momento. Cualquier cambio que pueda afectar al nivel de seguridad establecido deberá ser aprobado por el foro de gestión de EC.
d) Los controles de seguridad y procedimientos operativos para las instalaciones de la EC, sistemas e información necesarios para los servicios de certificación serán documentados, implementados y mantenidos.
e) La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se mantendrá la seguridad de información cuando la responsabilidad respecto a funciones de la EC haya sido subcontratada a otra organización.

Clasificación y gestión de información y bienes

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que sus activos y su información reciben un nivel de protección adecuado. En particular, la EC mantendrá un inventario de toda la información y hará una clasificación de los mismos y sus requisitos de protección en relación con el análisis de sus riesgos.

Operaciones de gestión

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los sistemas de la EC son seguros, son tratados correctamente, y con el mínimo riesgo de fallo. En particular:

a) se protegerá la integridad de los sistemas de EC y de su información contra virus y software malintencionado o no autorizado.
b) los daños derivados de incidentes de seguridad y los errores de funcionamiento deberán ser minimizados por medio del uso de reportes de incidencias y procedimientos de respuesta.
c) Los soportes serán custodiados de manera segura para protegerlos de daños, robo y accesos no autorizados.
d) Se establecerán e implementarán los procedimientos para todos los roles administrativos y de confianza que afecten a la prestación de servicios de certificación.

Tratamiento de los soportes y seguridad

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

Planning del sistema

f) Se deberá controlar la capacidad de atención a la demanda y la previsión de futuros requisitos de capacidad para asegurar la disponibilidad de recursos y de almacenamiento.

Reportes de incidencias y respuesta

g) La EC responderá de manera inmediata y coordinada para dar respuesta rápidamente a los incidentes y para reducir el impacto de los fallos de seguridad. Todos los incidentes serán reportados con posterioridad al incidente tan pronto como sea posible.

Procedimientos operacionales y responsabilidades

h) Las operaciones de seguridad de la EC serán separadas de las operaciones normales.

Gestión del sistema de acceso

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas. En particular:

- **EC General**

a) Se implementarán controles (p. Ej. Firewalls) para proteger la red interna de redes externas accesibles por terceras partes.
b) Los datos sensibles serán protegidos cuando estos sean transmitidos por redes no protegidas.
c) La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la efectiva administración de acceso de Partes Usuarias (incluyendo operadores, administradores y cualquier Parte Usuaria que confía que tenga un acceso directo al sistema) para mantener el sistema de seguridad, incluida la gestión de cuentas de Partes Usuarias, auditorías y modificación o supresión inmediata de accesos.
d) La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso a la información y a las funciones del sistema está restringido de acuerdo con la política de control de accesos, y que el sistema de la EC dispone de los controles de seguridad suficientes para la separación de los roles de confianza identificados en la DPC, incluyendo la separación del administrador de seguridad y las funciones operacionales. Concretamente, el uso de utilidades del sistema estará restringido y estrictamente controlado.
e) El personal de la EC identificado y autenticado antes de usar aplicaciones críticas relativas a la gestión de certificados.
f) El personal de la EC será responsable de sus actos, por ejemplo, por retener logs de eventos.
g) Se protegerán los datos sensibles contra medios de almacenamiento susceptibles de que la información sea recuperada y accesible por personas no autorizadas.

- **Generación del certificado**

h) La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los componentes de la red local (p. ej. routers) están guardados en un medio físico seguro y sus configuraciones son periódicamente auditadas
i) Las instalaciones de la EC estarán provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

- **Gestión de la revocación**

j) Las instalaciones de la EC estarán provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado o irregular.

Gestión del ciclo de vida del hardware criptográfico

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la seguridad del hardware criptográfico a lo largo de su ciclo de vida. En particular, que:

a) el hardware criptográfico de firma de certificados no se manipula durante su transporte.
b) el hardware criptográfico de firma de certificados no se manipula mientras está almacenado.
c) el uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.
d) el hardware criptográfico de firma de certificados está funcionando correctamente; y;
e) la clave privada de firma de la EC almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

7.8.3. Evaluación de la seguridad del ciclo de vida

La evaluación de la seguridad del ciclo de vida está supeditada a la metodología interna de la EC.

7.9. Controles de seguridad de la red

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

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos TLS.

7.10. Controles de ingeniería de los módulos criptográficos

Todas las operaciones criptográficas de la EC deben ser desarrolladas en un módulo validado por al menos el nivel 3 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente.

8. Perfiles de certificado y CRL

8.1. Perfil de certificado

Todos los certificados emitidos bajo esta política serán conformes a:

- Estándar X.509 versión 3
- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL profile”.

Y aquellos que son cualificados con:

- ETSI EN 319 412-2 v2.1.1 “Certificate Profiles-Part 2 Certificate profile for certificates issued to natural persons”

8.1.1. Número de versión

Deberá indicarse en el campo versión que se trata de la v.3.

8.1.2. Extensiones del certificado

El perfil del certificado está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.

8.1.3. Extensiones específicas

El certificado, emitido bajo la presente Política, podrá incluir por petición del suscriptor extensiones adicionales con información específica de su propiedad. Esta información estará bajo la exclusiva responsabilidad del suscriptor. Dichas extensiones no se marcarán como críticas y sean reconocibles como tales.

8.1.4. Identificadores de objeto (OID) de los algoritmos

Identificadores de objeto (OID) de los algoritmos criptográficos:

- SHA-1 With RSA Encryption (1.2.840.113549.1.1.5)
- SHA-256 With RSA Encryption (1.2.840.113549.1.1.11)

8.1.5. Formato de nombres

No estipulado.

8.1.6. Restricciones de los nombres

No estipulado.

8.2. Perfil de CRL y extensiones

Se soporta y se utilizan CRL conforme al estándar X.509.

8.3. OCSP Profile

8.3.1. Número de versión

Los certificados de respondedor OCSP son emitidos por cada EC gestionada por EC Camerfirma según el estándar RFC 6960.

8.3.2. Extensiones OCSP

El perfil del certificado de OCSP está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.

9. Especificación de la administración

9.1. Autoridad de las políticas

El departamento jurídico constituye la autoridad de las políticas (PA) y es responsable de la administración de las políticas.

9.2. Procedimientos de especificación de cambios

Cualquier elemento de esta política es susceptible de ser modificado.

Todos los cambios realizados sobre las políticas serán inmediatamente publicados en la web de Camerfirma.

En la web de Camerfirma se mantendrá un histórico con las versiones anteriores de las políticas.

Los terceros que confían afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la PA.

Si un cambio en la política afecta de manera relevante a un número significativo de terceros que confían de la política, la PA puede discrecionalmente asignar un nuevo OID a la política modificada.

9.3. Publicación y copia de la política

Una copia de esta política estará disponible en formato electrónico en una dirección de Internet definida en la DPC.

9.4. Procedimientos de aprobación de la DPC

Para la aprobación y autorización de una EC se deberán respetar los procedimientos especificados por la PA. Las partes de la DPC de una EC que contenga información relevante en relación a su seguridad, toda o parte de esa DPC no estarán disponible públicamente.

10. Anexo I – Acrónimos

CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DSCF	Dispositivo seguro de creación de firma

DSADCF	Dispositivo seguro de almacén de datos de creación de firma
EC	Entidad de Certificación
ER	Entidad de Registro
FIPS	Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
ITU	International Telecommunications Union. Unión Internacional de Telecomunicaciones
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL-TLS	Secure Sockets Layer. Protocolo que permite la transmisión de información cifrada entre un navegador de Internet y un servidor. El protocolo TLS (seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL.
TCP/IP	Transmission Control. Protocol/Internet Protocol. Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

11.Anexo II – Definiciones

Entidad de Certificación	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Tercero que confía, vinculando una determinada clave pública con una persona.
Autoridad de Políticas	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y DPC.
Entidad de Registro	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
Certificación cruzada	El establecimiento de una relación de confianza entre dos EC's, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del suscriptor y es firmada por la EC.

Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada **datos de verificación de firma.**
Clave privada	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada **datos de creación de firma.** La clave privada de la EC será usada para firma de certificados y firma de CRL's
CPS	Conjunto de prácticas adoptadas por una Entidad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta (también referida como DPC o Declaración de Prácticas de Certificación).
CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la EC.
Datos de Activación	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada
DSADCF	*Dispositivo seguro de almacén de los datos de creación de firma.* Elemento software o hardware empleado para custodiar la clave privada del suscriptor de forma que solo él tenga el control sobre la misma.
DSCF	*Dispositivo Seguro de creación de firma*. Elemento software o hardware empleado por el suscriptor para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el suscriptor.
Entidad	Dentro del contexto de las políticas de certificación de Camerfirma Perú, aquella empresa u organización de cualquier tipo Titular del Certificado y que puede mantener un vínculo con el suscriptor (Atributo).
Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a) que los datos no han sido modificados (integridad). b) que la persona que firma los datos es quien dice ser (identificación). c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen).
Firma remota	Tecnología de firma digital que permite firmar documentos electrónicamente desde cualquier lugar y dispositivo con internet, sin necesidad de tokens USB, utilizando un servidor seguro en la nube.
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.

Política de certificación	Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes
Suscriptor	Dentro del contexto de las políticas de certificación de Camerfirma Perú, persona natural cuya clave pública es certificada por la EC y dispone de una privada válida para generar firmas digitales.
Tercero que confía	Dentro del contexto de las políticas de certificación de Camerfirma Perú, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado

Camerfirma PERÚ

Tinexta Infocert

think next,
trust now