POLÍTICA DE CERTIFICACIÓN



el árbol de las culturas

www.futuver.com

futuver®

INDICE

1. CONTROL DEL DOCUMENTO 7

1.1 ACTUALIZACIONES 7
1.2 CONTROL DE CAMBIOS 7
1.3 MANTENIMIENTO DEL DOCUMENTO 7
1.4 VALIDEZ 7
1.5 TRATAMIENTO Y CONFIDENCIALIDAD 7

2. IDENTIFICACIÓN DE POLÍTICAS 8

3. INTRODUCCIÓN 9

3.1 CONSIDERACIÓN INICIAL 9
3.2 GENERALIDADES 9
3.3 IDENTIFICACIÓN 10
3.4 COMUNIDAD Y ÁMBITO DE APLICACIÓN 11
3.4.1 Autoridad de Certificación (AC) 11
3.4.2 Autoridad de Registro (AR) 11
3.4.3 Autoridad de Políticas (AP) 11
3.4.4 Firmante ó Suscriptor 11
3.4.5 Tercero que confía 11
3.4.6 Solicitante 11
3.4.7 Entidad 12
3.4.8 Ámbito de Aplicación y Usos 12
3.4.9 Usos Prohibidos y no Autorizados 13
3.4.10 Objetivos 13
3.4.11 Alcances 13
3.4.12 Limitaciones 14
3.5 MEDIDAS DE PRIVACIDAD Y PROTECCIÓN DE DATOS 14
3.6 CONTACTO 14

4. CLÁUSULAS GENERALES 15

4.1 OBLIGACIONES 15
4.1.1 AC 15
4.1.2 AR 16
4.1.3 Solicitante 17
4.1.4 Firmante/Suscriptor 17
4.1.5 Tercero que confía 18
4.1.6 Entidad 18
4.1.7 Repositorio 18
4.2 RESPONSABILIDAD 18

4.2.1 Exoneración de responsabilidad *19*
4.3 RESPONSABILIDAD FINANCIERA. 19
4.4 INTERPRETACIÓN Y EJECUCIÓN 20
4.3.1 Legislación *20*
4.3.2 Notificación *20*
4.3.3 Procedimiento de resolución de disputas. *20*
4.5 TARIFAS 20
4.4.1 Tarifas de emisión de certificados y renovación. *20*
4.4.2 Tarifas de acceso a los certificados *20*
4.4.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados. *20*
4.4.4 Tarifas por el acceso al contenido de estas Políticas de Certificación *21*
4.6 PUBLICACIÓN Y REPOSITORIOS 21
4.5.1 Publicación de información de la AC *21*
4.5.1.1 Políticas y prácticas de certificación. 21
4.5.1.2 Términos y condiciones. 21
4.5.1.3 Difusión de los certificados. 21
4.5.2 Frecuencia de publicación *22*
4.5.3 Controles de acceso *22*
4.7 AUDITORIAS 22
4.6.1 Frecuencia de las auditorias *22*
4.6.2 Identificación y calificación del auditor *22*
4.6.3 Relación entre el auditor y la AC *22*
4.6.4 Tópicos cubiertos por la auditoria *23*
4.6.5 Auditoria en las Autoridades de Registro *23*
4.8 CONFIDENCIALIDAD 23
4.7.1 Tipo de información a mantener confidencial *23*
4.7.2 Tipo de información considerada no confidencial *23*
4.7.3 Divulgación de información de revocación de certificados *24*
4.7.4 Envío a la Autoridad Competente *24*
4.9 DERECHOS DE PROPIEDAD INTELECTUAL. 24

5. IDENTIFICACIÓN Y AUTENTICACIÓN 25

5.1 REGISTRO INICIAL 25
5.1.1 Tipos de nombres *25*
5.1.2 Reglas utilizadas para interpretar varios formatos de nombres *25*
5.1.3 Unicidad de los nombres *25*
5.1.4 Procedimiento de resolución de disputas de nombres *25*
5.1.5 Métodos de prueba de la posesión de la clave privada *25*
5.1.6 Autenticación de la identidad de una organización *25*
5.1.7 Autenticación de la identidad de un individuo *25*

5.1.8 Autenticación del vínculo existente entre la entidad y la persona física. 26
5.1.9 Procedimiento simplificado de emisión de certificados 26
5.1.10 Requerimientos aplicables a las AR's externas. 26
5.2 RENOVACIÓN DE LA CLAVE Y DEL CERTIFICADO 27
5.3 SOLICITUD DE REVOCACIÓN 27
6. REQUERIMIENTOS OPERACIONALES 28
6.1 SOLICITUD DE CERTIFICADOS 28
6.1.1 Registro 28
6.2 EMISIÓN DE CERTIFICADOS 29
6.4 ACEPTACIÓN DE CERTIFICADOS 29
6.5 REVOCACIÓN DE CERTIFICADOS 30
6.5.1 Aclaraciones previas 30
6.5.2 Causas de revocación y documentos justificativos. 30
6.5.3 Quién puede solicitar la revocación 31
6.5.4 Procedimiento de solicitud de revocación 31
6.5.5 Periodo de revocación 32
6.5.6 Frecuencia de emisión de CRL's 32
6.5.7 Requisitos de comprobación de CRL's 32
6.5.8 Disponibilidad de comprobación on-line de la revocación 32
6.5.9 Requisitos de la comprobación on-line de la revocación 33
6.6 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD 33
6.6.1 En particular 33
6.6.2 Registro 34
6.6.3 Generación del certificado 34
6.6.4 Entrega del dispositivo al Firmante/Suscriptor 34
6.6.5 Gestión de la revocación 35
6.6.6 Tipos de eventos registrados 35
6.6.7 Frecuencia de procesado de Logs 36
6.6.8 Periodos de retención para los Logs de auditoria 36
6.6.9 Protección de los Logs de auditoría 36
6.6.10 Procedimientos de backup de los Logs de auditoría 36
6.6.11 Análisis de vulnerabilidades. 36
6.7 ARCHIVO DE REGISTROS 36
6.7.1 Tipo de archivos registrados 36
6.7.2 Periodo de retención para el archivo 37
6.7.3 Protección del archivo 37
6.7.4 Procedimientos de backup del archivo 37
6.7.5 Procedimientos para obtener y verificar información archivada 37
6.8 CAMBIO DE CLAVE DE LA AC 38

6.9 RECUPERACIÓN EN CASO DE COMPROMISO DE LA CLAVE O DESASTRE 38
6.9.1 La clave de la AC se compromete 38
6.9.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre 38
6.10 CESE DE LA AC 38

7. CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL 40

7.1 CONTROLES DE SEGURIDAD FÍSICA 40
7.1.1 AC General 40
7.1.2 Generación de certificados, entrega del dispositivo del Firmante/Suscriptor y gestión de revocaciones. ... 40
7.1.3 Ubicación y construcción 41
7.1.4 Acceso físico 41
7.1.5 Alimentación eléctrica y aire acondicionado 41
7.1.6 Exposición al agua 41
7.1.7 Protección y prevención de incendios 41
7.1.8 Sistema de almacenamiento. 41
7.1.9 Eliminación de residuos 42
7.1.10 Backup externo 42
7.2 CONTROLES PROCEDIMENTALES 42
7.2.1 Roles de confianza 42
7.2.2 Número de personas requeridas por tarea 43
7.2.3 Identificación y autentificación para cada rol 43
7.3 CONTROLES DE SEGURIDAD DE PERSONAL 43
7.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación 43
7.3.2 AC General 43
7.3.3 Registro, generación de certificados y gestión de revocaciones 44
7.3.4 Procedimientos de comprobación de antecedentes 44
7.3.5 Requerimientos de formación 44
7.3.6 Requerimientos y frecuencia de la actualización de la formación 45
7.3.7 Sanciones por acciones no autorizadas 45
7.3.8 Requerimientos de contratación de personal 45
7.3.9 Documentación proporcionada al personal 45

8. CONTROLES DE SEGURIDAD TÉCNICA 46

8.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES. 46
8.1.1 Generación del par de claves de la AC 46
8.1.2 Generación del par de claves del Firmante/Suscriptor 46
8.1.3 Entrega de la clave privada al Firmante/Suscriptor 46
8.1.4 Entrega de la clave pública de la AC a los Terceros que confían 47
8.1.5 Tamaño y periodo de validez de las claves del emisor 47
8.1.6 Tamaño y periodo de validez de las claves del Firmante/Suscriptor 47

8.1.7 Hardware/software de generación de claves *48*
8.1.8 Fines del uso de la clave *48*
8.2 PROTECCIÓN DE LA CLAVE PRIVADA 48
8.2.1 De la AC *48*
8.2.2 Del Firmante/Suscriptor *49*
8.3 ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS 49
8.3.1 Control multipersona (n de entre m) de la clave privada *49*
8.3.2 Custodia de la clave privada. *49*
8.3.3 Copia de seguridad de la clave privada *50*
8.3.4 Archivo de la clave privada *50*
8.3.5 Introducción de la clave privada en el módulo criptográfico *50*
8.3.6 Método de activación de la clave privada *50*
8.3.7 Método de desactivación de la clave privada *50*
8.3.8 Método de destrucción de la clave privada *50*
8.4 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES 51
8.4.1 Archivo de la clave pública *51*
8.4.2 Periodo de uso para las claves públicas y privadas *51*
8.5 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) 51
8.6 CONTROLES DE SEGURIDAD INFORMÁTICA 52
8.6.1 Requerimientos técnicos de seguridad informática específicos *52*
8.7 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA. 52
8.7.1 Controles de desarrollo del sistema. *52*
8.7.2 Controles de gestión de la seguridad. *53*
8.7.2.1 Gestión de seguridad. 53
8.7.3 Clasificación y gestión de información y bienes *53*
8.7.4 Operaciones de gestión *53*
8.7.5 Tratamiento de los soportes y seguridad *54*
8.7.6 Planning del sistema *54*
8.7.7 Reportes de incidencias y respuesta *54*
8.7.8 Procedimientos operacionales y responsabilidades *54*
8.7.9 Gestión del sistema de acceso *54*
8.7.10 AC General *55*
8.7.11 Generación del certificado *55*
8.7.12 Gestión de la revocación *56*
8.7.13 Gestión del ciclo de vida del hardware criptográfico *56*
8.7.15 Controles de seguridad de la red *56*
8.7.16 Controles de ingeniería de los módulos criptográficos *56*
9. PERFILES DE CERTIFICADO Y CRL 57

9.1 PERFIL DE CERTIFICADO 57
9.1.1 Número de versión *57*
9.1.2 Extensiones del certificado *57*
9.1.3 Identificadores de objeto (OID) de los algoritmos *57*
9.2 PERFIL DE CRL 57
9.2.1 Número de versión *57*
10. ESPECIFICACIÓN DE LA ADMINISTRACIÓN 58
10.1 AUTORIDAD DE LAS POLÍTICAS 58
10.2 PROCEDIMIENTOS DE ESPECIFICACIÓN DE CAMBIOS 58
10.3 PUBLICACIÓN Y COPIA DE LA POLÍTICA 58
10.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC 58

1. CONTROL DEL DOCUMENTO

1.1 Actualizaciones

VERSIÓN	FECHA	ELABORADO	ACTUALIZACIÓN	REVISADO	APROBADO
1.1	Mayo 2011	Luis Alberto García Gutiérrez	Luis Alberto García Gutiérrez	Luis Alberto García Gutiérrez	Luis Alberto García Gutiérrez

1.2 Control de cambios

DESCRIPCIÓN DEL CAMBIO	
AÑADIDO	
MODIFICADO	OID
ELIMINADO	

1.3 Mantenimiento del documento

Cada vez que haya cambios, es necesario publicar su actualización en la página web de Futuver.

1.4 Validez

Hasta su actualización.

1.5 Tratamiento y confidencialidad

Este documento es de uso público.

2. IDENTIFICACIÓN DE POLÍTICAS

La forma de identificar distintos tipos de certificados digitales es a través de identificadores de objeto (OID's). Un OID concreto permite a las aplicaciones distinguir claramente el certificado que se presenta.

El identificador de política está compuesto por una serie de números separados entre sí por puntos y con un significado concreto de cada uno de ellos. Dentro de un mismo tipo de certificados podemos definir diferentes subtipos en función a algunas características especiales.

En concreto, para este tipo de certificados distinguimos dentro del tipo genérico de certificados FUTUVER de persona física de vinculación de pertenencia a entidad, varios subtipos de certificados en función del atributo, del soporte de almacenamiento de las claves, así como de la entidad que genera las claves (el propio Firmante/Suscriptor o el prestador de servicios.

El siguiente cuadro muestra las diferentes variables respecto a los certificados emitidos por la AC FUTUVER:

Base : 1.3.6.1.4.1.37942.10.1

	AC	TITULAR	SOPORTE	GENERACIÓN	
AC FUTUVER	1	1			Certificado de Autoridad Certificadora FUTUVER
FUTUVER-CPN-SW-KUSU	1	2	1	2	Certificado FUTUVER de persona física de vinculación de pertenencia a empresa, claves almacenadas en software y generadas por el titular
FUTUVER-CPN-HW-KUSU	1	2	2	2	Certificado FUTUVER de persona física de vinculación de pertenencia a empresa, claves almacenadas en hardware y generadas por el titular

3. INTRODUCCIÓN

3.1 Consideración Inicial

Por no haber una definición taxativa de los conceptos de Declaración de Practicas de Certificación y Políticas de Certificación y debido a algunas confusiones formadas, entendemos que es necesario informar de su posición frente a estos conceptos.

Política de Certificación es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/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 Practicas de Certificación es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación 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 Firmante/Suscriptor o Tercero que confía y la Autoridad 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 Practicas de Certificación son distintos, pero aún así es muy importante su interrelación.

Una DPC detallada no forma una base aceptable para la interoperabilidad de Autoridades 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 "**que**" requerimientos de seguridad son necesarios para la emisión de los certificados. La DPC nos dice "**como**" se cumplen los requerimientos de seguridad impuestos por la política.

3.2 Generalidades

El presente documento especifica la Política de Certificación para el certificado de persona física de vinculación de pertenencia a entidad emitidos por la Autoridad de certificación **FUTUVER S.A. de C.V.** (en adelante Futuver), y está basada en la especificación del estándar RCF 2527 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, de IETF y del ETSI TS 102 042.

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

Esta política define las reglas y responsabilidades que deben seguir aquellas Autoridades de certificación que deseen emitir el tipo de certificado definido en el presente documento, imponiendo además ciertas obligaciones que deben ser tomadas en cuenta por los Firmantes/Suscriptores y Terceros que confían en virtud de su especial relación con este tipo de certificados.

De esta forma, cualquier AR 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 Firmantes/Suscriptores de su existencia.

La actividad de la AC podrá ser sometida a la inspección de la Autoridad de las Políticas (AP) o por personal delegado por la misma.

En lo que se refiere al contenido de esta Política de Certificación, 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.

3.3 Identificación

La presente Política de Certificación está identificada con el OID:

1.3.6.1.4.1.37942.10.1

1	Iso
3	Org
6	Dod
1	Internet
4	Private
1	Enterprise
37942	FUTUVER
10	Políticas de certificación
1	ESTAS POLITICAS

Dependiendo del tipo de certificado (ver apartado “Identificación de Políticas” de este documento):

- Certificado de persona física con atributo de vinculación a empresa (certificado de pertenencia ó de representante de empresa).

3.4 Comunidad y Ámbito de Aplicación

3.4.1 Autoridad de Certificación (AC)

Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Firmante/Suscriptor y el Tercero que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una persona física (Firmante/Suscriptor).

El emisor de este tipo de certificados es FUTUVER.

3.4.2 Autoridad de Registro (AR)

Ente que actúa conforme esta Política de Certificación y, en su caso, mediante acuerdo suscrito con la AC, cuyas funciones son la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado.

3.4.3 Autoridad de Políticas (AP)

Es el departamento jurídico de Futuver cuya función es inspeccionar cuando así sea necesario a la AC.

3.4.4 Firmante ó Suscriptor

Bajo esta Política el Firmante ó Suscriptor es la propia persona física, que en su caso, ostenta el atributo vinculación a la Entidad, titular y poseedora de un dispositivo de creación de firma con un Certificado.

3.4.5 Tercero que confía

En esta Política se entiende por Tercero que confía la persona física ó jurídica que voluntariamente confía en el certificado emitido a favor del emisor, lo utiliza como medio de acreditación de la autenticidad e integridad de la información firmada y en consecuencia se sujeta a lo dispuesto en esta Política, por lo que no se requerirá acuerdo posterior alguno.

3.4.6 Solicitante

Se entenderá por Solicitante, la persona física que solicita un Certificado emitido bajo esta Política.

El Solicitante puede ser distinto del suscriptor en los casos de certificados solicitados por un representante de una empresa para sus empleados o de un colectivo para sus afiliados. En el caso

de solicitud de un certificado de persona física para su propia representación, el concepto solicitante y suscriptor será el mismo.

3.4.7 Entidad

Bajo esta Política, la Entidad es la persona jurídica u organización a la que el Firmante/Suscriptor se encuentra estrechamente relacionado mediante la condición acreditada en el atributo: Una relación de vinculación de pertenencia a dicha Entidad.

La Entidad deberá solicitar la revocación del certificado cuando cese la vinculación del Firmante/Suscriptor con la organización.

3.4.8 Ámbito de Aplicación y Usos

Todos los certificados emitidos bajo esta Política, son válidos para asumir, por parte del Firmante/Suscriptor, responsabilidades, compromisos o derechos en su propio nombre, y en su caso, también en nombre de la Entidad en la medida en que se deduzca por la propia naturaleza del atributo del certificado.

Los Certificados emitidos bajo esta Política pueden ser utilizados con los siguientes propósitos:

Identificación del Firmante/Suscriptor: El Firmante/Suscriptor del Certificado 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/Suscriptor 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 integro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Firmante/Suscriptor. Se certifica que el mensaje recibido por el Tercero que confía es el mismo que fue emitido por el Firmante/Suscriptor.

No repudio de origen: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Firmante/Suscriptor que ha firmado no puede negar la autoría o la integridad del mismo.

A pesar de ser posible su utilización para el cifrado de datos, la AC no se responsabiliza por esta actividad, debido a que, por motivos de seguridad, esta Política determina que la AC no guarde copia de la clave privada del Firmante/Suscriptor. No se garantiza, por tanto, la recuperación de los datos cifrados en caso de pérdida de la clave privada por parte del Firmante/Suscriptor, el Firmante/Suscriptor o el Tercero que confía lo hará, en todo caso, bajo su propia responsabilidad.

Los usos tienen un carácter técnico pero se pueden incorporar usos específicos del certificado es decir "solo para realizar trámites con la SE" siempre que estos límites se indiquen en el certificado. Por lo tanto el usuario del certificado o parte confiante debe comprobar que la transacción realizada con el certificado esta dentro de los limites de uso del certificado.

3.4.9 Usos Prohibidos y no Autorizados

Los certificados emitidos bajo la presente Política 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 el propio contenido del certificado, la DPC y los Contratos de la AC con sus Firmantes/Suscriptores tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la AC, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el Firmante/Suscriptor o cualquier tercero.

En función de los servicios prestados por la AC mediante la emisión de sus certificados, no es posible por parte de la AC 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 AC.

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

Asimismo, le será imputable al Firmante/Suscriptor cualquier responsabilidad que pudiese derivarse de la utilización de cualquiera de los Certificados emitidos bajo esta política fuera de los límites ó condiciones de uso establecidas en el propio contenido del Certificado, en la DPC y los contratos de la AC con sus Firmantes/Suscriptores, así como de cualquier otro uso indebido del mismo derivado o que pueda ser interpretado como tal en función de la legislación vigente.

3.4.10 Objetivos

Asociar a un firmante/Suscriptor con una entidad en el marzo de sus funciones.

Garantizar el no repudio.

Garantizar la certeza respecto a la voluntad del firmante.

3.4.11 Alcances

Todos los alcances otorgados por las leyes aplicables referentes a la Firma Electrónica Avanzada.

3.4.12 Limitaciones

Establecidas en la DPC.

3.5 Medidas de privacidad y protección de datos

Futuver resguarda toda la información privada del firmante/solicitante bajo las disposiciones establecidas por la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

3.6 Contacto

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

E-mail:	ap@acfutuver.com
Teléfono:	52 80 59 91
Fax:	52 80 59 13
Dirección:	Campos Elíseos #345 Col. Polanco C.P. 1150 México D.F.

4. CLÁUSULAS GENERALES

4.1 Obligaciones

4.1.1 AC

La AC 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. Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
6. Revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL.
7. Informar a los Firmantes/Suscriptores de la revocación de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.
8. Publicar esta Política y sus Prácticas de Certificación correspondientes en la página Web.
9. Informar sobre las modificaciones de esta Política y de su Declaración Prácticas de Certificación a los Firmantes/Suscriptores y AR's que estén vinculadas a ella.
10. No almacenar ni copiar los datos de creación de firma del Firmante/Suscriptor.
11. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.
12. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante perdida o destrucción o falsificación

13. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

14. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualquier circunstancia pertinente para la emisión de los Certificados.

15. Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica;

16. Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad;

17. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación;

18. En el caso de cesar en su actividad, comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos;

19. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;

4.1.2 AR

Las AR'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. Pedir la documentación al solicitante de la emisión del certificado.

3. Comprobar la identidad de los solicitantes de certificados.

4. Verificar la exactitud y autenticidad de la información suministrada por el Firmante/Suscriptor solicitante.

5. Exhibir el contrato y pedir al solicitante su firma de conformidad.

6. Hacer mención de la política de seguridad al solicitante.

7. Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Firmante/Suscriptor.

8. Respetar lo dispuesto en los contratos firmados con la AC y con el Firmante/Suscriptor.

9. Recibir la solicitud de revocación del firmante mencionando las causas que la originaron.

10. Informar a la AC las causas de revocación.

11. Revocar certificado.

4.1.3 Solicitante

El solicitante de un Certificado estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

1. Suministrar a la AR la información necesaria para realizar una correcta identificación.

2. Confirmar la exactitud y veracidad de la información suministrada y firmar el contrato correspondiente.

3. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

4.1.4 Firmante/Suscriptor

El Firmante/Suscriptor 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. Respetar lo dispuesto en el contrato firmado con la Autoridad 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 período de validez.

4.1.5 Tercero que confía

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y además:

1. Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.

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.

4.1.6 Entidad

Será obligación de la Entidad solicitar a la AR la revocación del certificado cuando cese o se modifique la vinculación del Firmante/Suscriptor con la Entidad.

4.1.7 Repositorio

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

La AC 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.

4.2 Responsabilidad

La AC dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente.

La AC 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 Firmante/Suscriptores y de los terceros que confíen en los certificados.

Las responsabilidades de la AC incluyen las establecidas por la presente Política de Certificación, así como las que resulten de aplicación como consecuencia de la normativa Mexicana.

La AC será responsable del daño causado ante el Firmante/Suscriptor 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 Firmante/Suscriptor, 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 por la legislación vigente.

4.2.1 Exoneración de responsabilidad

La AC y las AR'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/Suscriptor o Terceros que confían 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/Suscriptor.

9. Fraude en la documentación presentada por el solicitante.

4.3 Responsabilidad Financiera.

La Ac asume la responsabilidad financiera, por los daños y prejuicios que puedan ocasionar a los usuarios de sus servicios siempre y cuando sea en caso de culpa o negligencia por parte de futuver, para lo cual dispone de un seguro de responsabilidad civil.

4.4 Interpretación y ejecución

4.3.1 Legislación

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por:

1. El Código de Comercio.
2. El Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.
3. Las Reglas Generales a las que Deberán Sujetarse los Prestadores de Servicios de Certificación.
4. Las demás leyes que resulten aplicables.

4.3.2 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 contacto.

4.3.3 Procedimiento de resolución de disputas.

Toda controversia o conflicto que se derive del presente documento, se resolverá mediante las leyes Mexicanas.

4.5 Tarifas

La AC se reserva el derecho de imponer alguna tarifa para la realización de los servicios como AC.

4.4.1 Tarifas de emisión de certificados y renovación.

Los precios de los servicios de certificación o cualquier otro servicio relacionado estarán disponibles para los Terceros que confían en la dirección Internet de la AC.

4.4.2 Tarifas de acceso a los certificados.

El acceso a los certificados emitidos es gratuito.

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

La AC proveerá acceso a la información relativa al estado de los certificados o de los certificados revocados de forma gratuita.

4.4.4 Tarifas por el acceso al contenido de estas Políticas de Certificación

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

4.6 Publicación y repositorios

4.5.1 Publicación de información de la AC

4.5.1.1 Políticas y prácticas de certificación.

La AC estará obligada a publicar la información relativa a sus Políticas y Prácticas de Certificación.

La presente Política de Certificación es pública y estará disponible en la dirección Internet de la AC.

Las Prácticas de Certificación de referencia serán así mismo públicas y se pondrán a disposición del público en la dirección Internet de la AC.

4.5.1.2 Términos y condiciones.

La AC o la AR pondrán a disposición de los Firmantes/Suscriptores y Terceros que confían los términos y condiciones del servicio antes de proceder a la emisión del certificado o de entregar los datos de activación de la clave privada.

4.5.1.3 Difusión de los certificados.

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son accesibles para los Firmantes/Suscriptores y Terceros que confían.

En concreto:

a) El certificado de la AC es público y se encontrará disponible en la dirección Internet de la AC .

b) El resto de los certificados estarán disponibles al público en la dirección Internet de la AC sólo en los casos en que el Firmante/Suscriptor haya otorgado su consentimiento

c) La AC pondrá a disposición de los Terceros que confían los términos y condiciones referentes al uso de los certificados

d) En caso de fallo del sistema u otros factores que no se encuentran bajo el control de la AC, la AC hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de **24 horas**.

4.5.2 Frecuencia de publicación

Las Políticas y Prácticas de Certificación se publicarán una vez hayan sido creadas.

La AC publicará los certificados revocados 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 de usuarios se publicará con una frecuencia diaria.

4.5.3 Controles de acceso

El acceso a la información será gratuito y estará a disposición de los Firmantes/Suscriptores y Terceros que confían.

La AC podrá establecer sistemas de seguridad para controlar el acceso a la información contenida en la Web, LDAP o CRL con el fin de evitar usos indebidos que afecten a la protección de datos personales.

4.7 Auditorias

4.6.1 Frecuencia de las auditorias

Se realizará una auditoria al menos cada seis meses, salvo que se establezca un plazo menor por la normativa vigente.

4.6.2 Identificación y calificación del auditor

El auditor debe poseer conocimientos y experiencia en sistemas de PKI y en seguridad de sistemas informáticos.

4.6.3 Relación entre el auditor y la AC

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

No obstante, lo anterior no impedirá la realización de auditorías internas periódicas.

4.6.4 Tópicos cubiertos por la auditoria

La auditoria deberá verificar en todo caso:

- Que la AC tiene un sistema que garantice la calidad del servicio prestado.
- Que la AC cumple con los requerimientos de esta Política de Certificación.
- Que las Prácticas de Certificación de la AC 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.

4.6.5 Auditoria en las Autoridades de Registro

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

4.8 Confidencialidad

4.7.1 Tipo de información a mantener confidencial

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

La AC 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 AC se abstendrá de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir dichas claves.

4.7.2 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/Suscriptor 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.

4.7.3 Divulgación de información de revocación de certificados

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

4.7.4 Envío a la Autoridad Competente

Se proporcionará la información solicitada mediante mandamiento expreso emitido por la autoridad competente en los casos y forma establecidos en la ley.

4.9 Derechos de propiedad Intelectual.

La propiedad intelectual de este documento pertenece a Futuver.

5. IDENTIFICACIÓN Y AUTENTICACIÓN

5.1 Registro inicial

5.1.1 Tipos de nombres

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

5.1.2 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.

5.1.3 Unicidad de los nombres

La AC 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 AC 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.

5.1.4 Procedimiento de resolución de disputas de nombres

Se atenderá a lo dispuesto en el apartado 4.3.3 de este documento.

5.1.5 Métodos de prueba de la posesión de la clave privada

Si el par de claves es generado por el Firmante/Suscriptor, la AC proveerá en la DPC la garantías que el suscriptor deberá aportar de estar en posesión de clave privada.

5.1.6 Autenticación de la identidad de una organización

En el caso de los 'Certificados de persona física de vinculación', emitidos bajo la presente Política, se identifica a una persona física vinculada a una Entidad, por lo que se exigirá, en todo caso, la acreditación de la existencia de la Entidad por un medio conforme a Derecho.

En el caso de los 'certificados de persona física' en los que no se da el atributo de vinculación a entidad, este requisito no se aplica.

5.1.7 Autenticación de la identidad de un individuo

En los certificados emitidos bajo esta Política, para realizar una correcta identificación de la identidad del firmante/suscriptor, se deberá atender a lo dispuesto por la legislación vigente, en

concreto, se exigirá la presencia física del mismo salvo en los casos que marque la legislación correspondiente.

5.1.8 Autenticación del vínculo existente entre la entidad y la persona física.

Entre la entidad y la persona física se deberá comprobar y documentar fehacientemente el vinculo.

En su caso, para autentificar el vínculo existente entre la entidad y la persona física, se deberá acreditar 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.

5.1.9 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/Suscriptor respecto de una solicitud anterior.

El Firmante/Suscriptor asumirá la responsabilidad mediante declaración firmada de la corrección de los datos no modificados. En los certificados de vinculación se comprobará que no exista una orden, por parte del representante suficiente de la entidad, contraria a la emisión del certificado.

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

5.1.10 Requerimientos aplicables a las AR's externas.

Cuando la AC emplee AR's externas deberá asegurar los siguientes aspectos:

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

5.2 Renovación de la clave y del certificado

La AC deberá informar al Firmante/Suscriptor antes de renovar de los términos y condiciones que hayan cambiado respecto de la anterior emisión.

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

Un certificado podrá ser renovado un numero limitado de veces. Las limitaciones de renovación estarán sujetas a la legislación vigente. Una vez trascurrido el plazo máximo de renovación el solicitante deberá proceder a una nueva solicitud..

La comparecencia del firmante/suscriptor puede no ser necesaria cuando la solicitud de renovación se realice de forma on-line por medio del certificado que se pretende renovar. No obstante lo anterior, se exigirá comparecencia siempre que hayan transcurrido más de 2 años desde la última verificación de la identidad realizada mediante la personación física del solicitante.

5.3 Solicitud de revocación

Todas las solicitudes de revocación deberán ser autenticadas.

6. REQUERIMIENTOS OPERACIONALES

6.1 Solicitud de certificados

La AC se asegurará que los Firmantes/Suscriptores están correctamente identificados y que la petición del certificado es completa.

6.1.1 Registro

a) Antes de comenzar una relación contractual, la AC, por sí misma o por medio de la AR, deberá informar al Firmante/Suscriptor 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 AC, por sí misma o por medio de la AR, deberá comprobar, de acuerdo con la legislación vigente, la identidad y los atributos específicos del Firmante/Suscriptor.

d) El Firmante/Suscriptor deberá facilitar su dirección física u otros datos que permitan contactar con él.

e) La AC, por sí misma o por medio de la AR, 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.

f) La AC, por sí misma o por medio de la AR, deberá guardar el contrato firmado con el Firmante/Suscriptor, el cual incluirá:

- Acuerdo de las obligaciones del Firmante/Suscriptor
- Compromiso del Firmante/Suscriptor a usar el dispositivo de creación de firma ofrecido por la AC de forma diligente
- Consentimiento para que la AC guarde la información usada para el registro, entrega del dispositivo del Firmante/Suscriptor, para una futura revocación, así como para el traspaso de información a una tercera parte en el caso de que la AC cese su actividad.

- Bajo qué condiciones el Firmante/Suscriptor consiente la publicación de su certificado.
- Que la información contenida en el certificado es correcta.

g) Los registros identificados deberán conservarse durante el periodo de tiempo que se indicó al Firmante/Suscriptor y que es necesario a efectos probatorios en los procedimientos legales.

h) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el Firmante/Suscriptor está en posesión de la clave privada asociada a la clave pública.

i) La AC por sí misma o por medio de la AR, deberá cumplir con todos los requisitos impuestos por la legislación aplicable en materia de protección de datos.

6.2 Emisión de certificados

La AC deberá poner todos los medios a su alcance para asegurar que la emisión y renovación de certificados se realiza de una forma segura. En particular:

- Cuando se generen las claves del Firmante/Suscriptor, que el procedimiento de emisión del certificado está ligado de manera segura a la generación del par de claves.
- La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los DN asignados a los Firmantes/Suscriptores.
- La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados con el Firmante/Suscriptor o entre distintos componentes del sistema de certificación.
- La AC deberá verificar que el registro de los datos es intercambiado con proveedores de servicios reconocidos, cuya identidad es autenticada.
- La AC deberá notificar al Solicitante de la emisión de su certificado.
- Dicha emisión se realiza en territorio Nacional.

6.4 Aceptación de certificados

La entrega del certificado y la firma del contrato de adhesión al sistema de certificación implicarán la aceptación del certificado por parte del Firmante/Suscriptor.

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

No obstante, a partir de la entrega del certificado, el Firmante/Suscriptor dispondrá de un periodo de siete 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 AC y el contenido del certificado, ello deberá ser comunicado de inmediato a la AC para que proceda a su revocación y a la emisión de un nuevo certificado.

La AC entregará el nuevo certificado sin coste para el Firmante/Suscriptor en el caso de que la diferencia entre los datos sea causada por un error no imputable al Firmante/Suscriptor. Transcurrido dicho periodo sin que haya existido comunicación, se entenderá que el Firmante/Suscriptor ha confirmado la aceptación del certificado y de todo su contenido.

Aceptando el certificado, el Firmante/Suscriptor confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la AR, la AC o cualquier tercero que de buena fe confíe en el contenido del Certificado.

6.5 Revocación de certificados

6.5.1 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 del mismo. Al hablar de revocación nos referiremos siempre a la pérdida de validez definitiva.

Por tanto, a efectos de la presente política de certificación, hablaremos de revocación para referirnos a aquella revocación de carácter definitivo.

6.5.2 Causas de revocación y documentos justificativos.

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

- Solicitud voluntaria del Firmante/Suscriptor o del solicitante.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del Firmante/Suscriptor o incapacidad sobrevenida, total o parcial.
- 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/Suscriptor o de la AC han sido comprometidas, bien porque concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
- Por incumplimiento por parte de la AR, AC o el Firmante/Suscriptor de las obligaciones establecidas en esta política.
- Por el término del contrato con el Firmante/Suscriptor.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la presente política.

6.5.3 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse únicamente por el Firmante/Suscriptor o por la propia AC. No obstante, en el caso de 'Certificado de persona física de vinculación' la revocación también podrá solicitarse por un representante de la entidad a la que pertenece o a la que está vinculado.

6.5.4 Procedimiento de solicitud de revocación

La AC 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 estará disponible para todos los Terceros que confían. Este deberá ser como máximo de 6 horas

El Firmante/Suscriptor cuyo certificado haya sido revocado deberá ser informado del cambio de estado de su certificado. Así mismo, el Firmante/Suscriptor deberá ser informado del levantamiento de la revocación. La AC 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 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 estas serán publicadas al menos semanalmente.

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

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 AC, la AC 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.

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.

6.5.5 Periodo de revocación

La decisión de revocar o no un certificado no podrán retrasarse por un periodo máximo de 7 días naturales.

6.5.6 Frecuencia de emisión de CRL's

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

La AC actualizará y publicará la CRL de acuerdo a los tiempos establecidos en la DPC, después de la recepción de una solicitud que haya sido previamente validada y al menos con una frecuencia diaria si no se han producido cambios en la CRL.

6.5.7 Requisitos de comprobación de CRL's

Los Terceros que confían podrán comprobar el estado de los certificados en los cuales va a confiar, debiendo comprobar en todo caso la última CRL emitida.

6.5.8 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 AC, la AC 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.

6.5.9 Requisitos de la comprobación on-line de la revocación

El Tercero que confía que desee comprobar la revocación de un certificado, podrá hacerlo de forma on-line a través de la dirección Internet de la AC.

La AC dispondrá de un sistema de consulta que impida la obtención masiva de datos relativos a los Firmantes/Suscriptores, 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.

6.6 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. En particular:

6.6.1 En particular

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 AC

6.6.2 Registro

a. La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que todos los eventos relativos al registro, incluyendo las peticiones de renovación y revocación serán registrados.

b. La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relativa al registro es almacenada, incluyendo la siguiente:

   - La documentación presentada por el solicitante para el registro.
   - Copia de documentos identificativos (Credencial para votar con Fotografía otorgada por el Instituto Federal Electoral o pasaporte o cédula profesional, Clave Única de Registro de Población y Registro Federal de Contribuyentes,) y el contrato suscrito con el Firmante/Suscriptor.
   - Algunas cláusulas específicas contenidas en el contrato (p.ej. el consentimiento de la publicación del certificado).
   - Método empleado para comprobar la validez de los documentos identificativos, si existe.
   - Nombre de la Autoridad de Registro.

c. La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la privacidad de la información relativa al Firmante/Suscriptor.

6.6.3 Generación del certificado

a. La AC registrará todos los eventos relativos al ciclo de vida de las claves de la AC.

b. La AC registrará todos los eventos relativos al ciclo de vida de los certificados.

6.6.4 Entrega del dispositivo al Firmante/Suscriptor

a. La AC registrará todos los eventos relativos al ciclo de vida de las claves de los Firmantes/Suscriptores generadas.

6.6.5 Gestión de la revocación

a. La AC 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.

6.6.6 Tipos de eventos registrados

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

La AC registrará y guardará los logs de todos los eventos relativos al sistema de seguridad de la AC. Estos incluirán eventos como:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las Aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificación.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Intentos de dar de alta, eliminar, habilitar y deshabilitar Firmantes/Suscriptores y actualizar.
- Cambios personales.

6.6.7 Frecuencia de procesado de Logs

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

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

6.6.8 Periodos de retención para los Logs de auditoria

La información almacenada deberá ser conservada durante el tiempo marcado por la legislación vigente o en su caso por una duración no menor a 10 años.

6.6.9 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.

6.6.10 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.

6.6.11 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 anual.

6.7 Archivo de registros

6.7.1 Tipo de archivos registrados

Los siguientes datos y archivos deben ser almacenados por la AC 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 AC es responsable del correcto archivo de todo este material

6.7.2 Periodo de retención para el archivo

La información detallada en el apartado 6.6.2, 6.6.3 a) y b), los contratos con los Firmantes/Suscriptores y cualquier información relativa a la identificación y autenticación del Firmante/Suscriptor deberá ser conservada durante el tiempo marcado por la legislación vigente o durante al menos15 años.

6.7.3 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.

6.7.4 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.

6.7.5 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.

6.8 Cambio de clave de la AC

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

Los siguientes certificados serán puestos a disposición pública en el directorio:

Clave pública de la nueva AC firmada por la clave privada de la vieja AC.

Clave pública de la vieja AC firmada con la clave privada de la nueva AC.

6.9 Recuperación en caso de compromiso de la clave o desastre

La AC 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:

6.9.1 La clave de la AC se compromete

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

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

- Informar a todos los Firmantes/Suscriptores, Terceros que confían y otras ACs 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.

6.9.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre

La AC tiene un plan apropiado de contingencias para la recuperación en caso de desastres.

La AC debe reestablecer los servicios de acuerdo con esta política dentro de las 48 horas posteriores a un desastre o emergencia imprevista. Tal plan incluirá una prueba completa y periódica de la preparación para tal reestablecimiento.

6.10 Cese de la AC

La AC 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/Suscriptores o Terceros que

confían 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:

- Informar a todos los Firmantes/Suscriptores, Terceros que confían y otras AR´s con los cuales tenga acuerdos u otro tipo de relación del cese.
- La AC revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- La AC realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los Firmantes/Suscriptores y Terceros que confían.
- Las claves privadas de la AC serán destruidas deshabilitadas para su uso.

b) La AC 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:

- Informar a las entidades afectadas.
- Transferencia de las obligaciones de la AC a otras partes.
- Cómo debe ser tratada la revocación de certificados emitidos cuyo periodo de validez aun no ha expirado.

En particular, la AC deberá:

- Informar puntualmente a todos los Firmantes/Suscriptores, empleados, Terceros que confían y AR´s con una anticipación mínima de 3 meses antes del cese.
- Transferir todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación.

7. CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL

7.1 Controles de Seguridad física

La AC 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:

7.1.1 AC General

a) El acceso físico a las instalaciones vinculadas a la generación de certificados, entrega del dispositivo al Firmante/Suscriptor 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.

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

a) 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.

b) La protección física se conseguirá por medio de la creación de una sala de generación de certificados y gestión de revocaciones controladas por cámaras y alarmas de seguridad.

c) Los controles de seguridad física y medioambiental serán implementados para proteger las instalaciones que albergan los recursos del sistema, los recursos del sistema en si 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/Suscriptor 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.

d) 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.

7.1.3 Ubicación y construcción

Las instalaciones de la AC están 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.

7.1.4 Acceso físico

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

7.1.5 Alimentación eléctrica y aire acondicionado

La AC 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 AC.

7.1.6 Exposición al agua

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

7.1.7 Protección y prevención de incendios

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de AC está protegido con un sistema anti-incendios.

7.1.8 Sistema de almacenamiento.

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

7.1.9 Eliminación de residuos

La AC 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 AC serán destruidos, así como que la información que contengan será irrecuperable.

7.1.10 Backup externo

La AC 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.

7.2 Controles procedimentales

7.2.1 Roles de confianza

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

Los roles de confianza incluyen las siguientes responsabilidades:

- **Profesional Jurídico:** Asume la responsabilidad de cuestiones legales regidas por el código de comerco, el reglamento del código de comercio, las reglas a las que deberán sujetarse los Prestadores de Servicio de Certificación y todas aquellas jurisprudencias que abarquen temas de firma electrónica.
- **Profesional Informático:** Asume la responsabilidad de cuestiones tecnológicas a las que se sujetan los Prestadores de Servicios de Certificación.
- **Oficial 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 de 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. Funciones de apoyo en el control dual de las operaciones de la AC.

- **Administrador de AC:** Responsable de la Administración y control de gestión de los sistemas de confianza de la AC.
- **Administrador de redes:** Asume la responsabilidad de mantener un alta disponibilidad en las comunicaciónes de la AC.
- **Administrador de Bases de Datos:** Asume la responsabilidad de gestionar las bases de datos de la AC.
- **Auditor de AC:** Realiza las labores de supervisión y control de la implementación de las políticas de seguridad.

7.2.2 Número de personas requeridas por tarea

Las siguientes tareas requerirán al menos un control dual:

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

7.2.3 Identificación y autentificación para cada rol

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

7.3 Controles de seguridad de personal

7.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

La AC 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:

7.3.2 AC General

a) La AC 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 AC, serán documentadas en la descripción del trabajo.

c) Se deberá describir el trabajo del personal de la AC (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 especificas de la AC.

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.

7.3.3 Registro, generación de certificados y gestión de revocaciones

a) 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.

b) Todo el personal implicado en roles de confianza deberá estar libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de la AC.

c) El personal de la AC será formalmente designado para desempeñar roles de confianza por el oficial de seguridad.

d) La AC 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.

7.3.4 Procedimientos de comprobación de antecedentes

La AC 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 AC que propicie la confianza suficiente en el empleado. Se entenderá como experiencia necesaria el haber pertenecido al Departamento en cuestión durante al menos 24 meses.

7.3.5 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 AC o AR, recibirá una formación relativa a:

- Los principales mecanismos de seguridad de AC y/o AR.

- Todo el software de PKI y sus versiones empleados en el sistema de la AC.
- Todas las tareas de PKI que se espera que realicen.
- Los procedimientos de resolución de contingencias y continuidad de negocio.

7.3.6 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.

7.3.7 Sanciones por acciones no autorizadas

Las posibles sanciones por la realización de acciones no autorizadas, están establecidas en la política de RRHH.

7.3.8 Requerimientos de contratación de personal

Ver el apartado 7.3.1.

7.3.9 Documentación proporcionada al personal

Todo el personal de la AC y AR deberá recibir los manuales de Tercero que confía en los que se detallen al menos los procedimientos para el registro de certificados, creación, actualización, renovación, revocación y la funcionalidad del software empleado.

8. CONTROLES DE SEGURIDAD TÉCNICA

8.1 Generación e instalación del par de claves.

8.1.1 Generación del par de claves de la AC

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

En particular:

a) La generación de la clave de la AC se realizará en un entorno securizado 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 AC se realizará en un dispositivo que cumpla los requerimientos que se detallan en el FIPS 140, en su nivel 3.

8.1.2 Generación del par de claves del Firmante/Suscriptor

Cuando las claves del Firmante/Suscriptor son generadas por el mismo, se generan de forma segura y 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 a la tecnologia para los propósitos de la firma electrónica avanzada y para el algoritmo de clave público empleado.

8.1.3 Entrega de la clave privada al Firmante/Suscriptor

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) o bien en un medio software (p. Ej. PKCS12).

Cuando la AC entrega un dispositivo seguro al Firmante/Suscriptor, 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 Tercero 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.

8.1.4 Entrega de la clave pública de la AC a los Terceros que confían

La AC 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 los Terceros que confían.

En particular:

a) La clave pública de la AC estará disponible a los Terceros que confían de manera que se asegure la integridad de la clave y se autentique su origen.

b) El certificado de la AC y su fingerprint (huella digital) estarán a disposición de los Terceros que confían a través de la página Web.

8.1.5 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 2048 bits para firmar certificados.

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

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

8.1.6 Tamaño y periodo de validez de las claves del Firmante/Suscriptor

El Firmante/Suscriptor deberá usar claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits.

El periodo de uso de la clave pública y privada del Firmante/Suscriptor 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.

8.1.7 Hardware/software de generación de claves

Las claves de la AC deberán ser generadas en un módulo criptográfico validado al menos por el nivel 3 de FIPS 140.

El par de claves y las claves simétricas para los Firmantes/Suscriptores serán generadas en un módulo de software y / o hardware criptográfico.

8.1.8 Fines del uso de la clave

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

La clave privada del Firmante/Suscriptor deberá ser usada para firma autenticación o cifrado según se describa en el contenido de dicho certificado, informándose en la correspondiente DPC como se identifica cada uso y si se permite más de un uso por certificado o se establecen certificados separados por cada uso.

8.2 Protección de la clave privada

8.2.1 De la AC

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

a) La clave privada de firma de la AC será mantenida y usada en un dispositivo criptográfico seguro, el cual cumple los requerimientos que se detallan en el FIPS 140, en su nivel 3.

b) Cuando la clave privada de la AC esté fuera del módulo criptográfico esta deberá estar protegida criptográficamente.

c) Se deberá hacer un back up de la clave privada de firma de la AC, 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.

d) Las copias de back up de la clave privada de firma de la AC se regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

8.2.2 Del Firmante/Suscriptor

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

- El Firmante/Suscriptor 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/Suscriptor contra un uso ajeno.

8.3 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.

8.3.1 Control multipersona (n de entre m) de la clave privada

Se requerirá un control multi-persona para la activación de la clave privada de la AC. 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.

8.3.2 Custodia de la clave privada.

La clave privada de la AC debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

En ningún caso la AC podrá almacenar la clave privada de firma del Firmante/Suscriptor.

Las claves de los Firmantes/Suscriptores estarán custodiadas por este ya sea en dispositivos software como en tarjeta criptográfica tal como se describe en el certificado digital asociados a estas.

8.3.3 Copia de seguridad de la clave privada

La AC deberá realizar una copia de backup 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.

8.3.4 Archivo de la clave privada

La clave privada de la AC no podrá ser archivada una vez finalizado su ciclo de vida.
Las claves privadas de Firmante/Suscriptor no pueden ser archivadas por la AC.

8.3.5 Introducción de la clave privada en el módulo criptográfico

La clave privada de la Autoridad de certificación debe crearse en el propio dispositivo. La inserción de la clave privada en el modulo criptográfico desde un fichero de copia debe realizarse en un entorno seguro y con un control dual.

8.3.6 Método de activación de la clave privada

La clave privada de la AC deberá ser activada conforme al apartado 8.3.1.

Se deberá proteger el acceso a la clave privada del Firmante/Suscriptor por medio de un password, PIN, u otros métodos de activación equivalentes. Si estos datos de activación deben ser entregados al Firmante/Suscriptor, 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/Suscriptor y no deben ser anotados en un lugar de fácil acceso ni compartidos.

8.3.7 Método de desactivación de la clave privada

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

8.3.8 Método de destrucción de la clave privada

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

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

La destrucción o deshabilitación de las claves se detallará en la DPC o en un documento creado al efecto.

Las claves privadas de los Firmantes/Suscriptores deberán ser destruidas o hacerlas inservibles después del fin de su ciclo de vida por el propio Firmante/Suscriptor.

8.4 Otros aspectos de la gestión del par de claves

8.4.1 Archivo de la clave pública

La AC deberá conservar todas las claves públicas de verificación

8.4.2 Periodo de uso para las claves públicas y privadas

Esta establecido en la DPC.

8.5 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 AC deberá, por si misma o por delegación de esta función, realizar los mayores esfuerzos que estén a su alcance 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 AC 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/Suscriptor.

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.

8.6 Controles de seguridad informática

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

- Identificación de todos los Terceros que confían.
- Controles de acceso basados en privilegios.
- Control dual para ciertas operaciones relativas a la seguridad.
- Generación de logs, revisión de auditoria y archivo de todos los eventos relacionados con la seguridad.
- Backup y recuperación.

8.6.1 Requerimientos técnicos de seguridad informática específicos

Cada servidor de AC incluirá las siguientes funcionalidades:

- Control de acceso a los servicios de AC 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/Suscriptor y la AC y datos de auditoria.
- Auditoria de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de la AC.
- Mecanismos de recuperación de claves y del sistema de AC.
- Las funcionalidades de arriba pueden ser provistas por el sistema operativo o mediante una combinación de sistemas operativos, software de PKI y protección física.

8.7 Controles de seguridad del ciclo de vida.

8.7.1 Controles de desarrollo del sistema.

La AC empleará sistemas fiables y productos que estén protegidos contra modificaciones.

8.7.2 Controles de gestión de la seguridad.

8.7.2.1 Gestión de seguridad.

La AC 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 AC 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 AC en los acuerdos concretos que la AC suscriba con esas terceras partes para asegurar que éstas están obligadas a implementar cualquier control requerido por la AC. La AC será responsable por la revelación de prácticas relevantes.

b) La AC 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 AC deberá mantenerse en todo momento. Cualquier cambio que pueda afectar al nivel de seguridad establecido deberá ser aprobado por el foro de gestión de AC.

d) La AC 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 AC haya sido subcontratada a otra organización.

8.7.3 Clasificación y gestión de información y bienes

La AC 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 AC mantendrá un inventario de toda la información y hará una clasificación de los mismos y sus requisitos de protección en relación al análisis de sus riesgos.

8.7.4 Operaciones de gestión

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

a) Se protegerá la integridad de los sistemas de AC 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.

8.7.5 Tratamiento de los soportes y seguridad

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

8.7.6 Planning del sistema

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.

8.7.7 Reportes de incidencias y respuesta

La AC 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

8.7.8 Procedimientos operacionales y responsabilidades

Las operaciones de seguridad de la AC serán separadas de las operaciones normales.

8.7.9 Gestión del sistema de acceso

La AC 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:

8.7.10 AC 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 AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la efectiva administración de acceso de Terceros que confían (incluyendo operadores, administradores y cualquier Tercero que confía que tenga un acceso directo al sistema) para mantener el sistema de seguridad, incluida la gestión de cuentas de Terceros que confían, auditorias y modificación o supresión inmediata de accesos.

d) La AC 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 AC 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 AC identificado y autenticado antes de usar aplicaciones críticas relativas a la gestión de certificados.

f) El personal de la AC 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.

8.7.11 Generación del certificado

La AC 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

Las instalaciones de la AC 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.

8.7.12 Gestión de la revocación

Las instalaciones de la AC 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.

8.7.13 Gestión del ciclo de vida del hardware criptográfico

La AC 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:

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.

e) La clave privada de firma de la AC almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo

8.7.15 Controles de seguridad de la red

Ya definido en la DPC.

8.7.16 Controles de ingeniería de los módulos criptográficos

Todas las operaciones criptográficas de la AC deben ser desarrolladas en un módulo validado por al menos el nivel 3 de FIPS 140.

9. PERFILES DE CERTIFICADO Y CRL

9.1 Perfil de Certificado

Todos los certificados emitidos bajo esta política serán compatibles al estándar ISO/IEC 9594-8, X.509 versión 3 y al RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", además de contener los datos del artículo 108 del código de comercio.

9.1.1 Número de versión

Deberá indicarse en el campo versión que se trata de la v.1.1

9.1.2 Extensiones del certificado

Las extensiones de los Certificados emitidos bajo esta Política se pueden incorporar en un documento adjunto de forma que se pueda gestionar de forma separada a este documento de políticas de certificación.

9.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma será 1.3.6.1.4.1.37942.10.1.1

El identificador de objeto del algoritmo de la clave pública será:

RsaEncryption 1. 2. 840. 113549. 1. 1. 1

9.2 Perfil de CRL

El perfil de la CRL se pueden incorporar en un documento adjunto de forma que se pueda getionar de forma separada a este documento de políticas de certificación.

9.2.1 Número de versión

Las CRL emitidas bajo esta política deberán ser v2.

10. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

10.1 Autoridad de las políticas

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

10.2 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 dirección Internet de FUTUVER.

En la dirección Internet de FUTUVER 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.

10.3 Publicación y copia de la política

Una copia de esta política estará disponible en formato electrónico en la dirección de Interne de la AC.

10.4 Procedimientos de aprobación de la DPC

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



España • Rumanía • México • Panamá

Edificio Futuver
Jimena Fdez. de la Vega, 55
Parque Científico Tecnológico
33203 Gijón - Asturias
España

T. +34 902 175 454 - F. +34 985 175 967

Edificio Registro de la Propiedad de Madrid
Futuver
c/ Alcalá 540
28027 Madrid
España

T. +34 911 295 454 - F. +34 901 706 175

www.futuver.com