POLÍTICA DE CERTIFICACIÓN

AVANSI c.x.a.

CERTIFICADO DE PERSONA FÍSICA CON VÍNCULO INSTITUCIONAL

Versión 2.0

Nombre:	Política de Certificación de Certificado de Persona Física con Vínculo Institucional
Código	PC-AVS-PF
Versión:	2.0
Elaborado por:	AVANSI C. por A.
Idioma:	Español
Descripción:	Define los criterios básicos a seguir por la CA que emita este tipo de certificados, por las RA's que pudieran utilizarlos y por los Firmantes/Suscriptores y terceros que confían en este tipo de certificados.
Fecha de edición:	20 de noviembre de 2006
Estado del documento:	Activo
Referencia (OID):	1.3.6.1.4.1.27395.6.2.1
Localización:	http://politicas.avansi.com.do

Control de versiones

VERSIÓN	MOTIVACIÓN DEL CAMBIO	PUBLICACIÓN
2.0	Cambios para implantación extensiva en República Dominicana	20/11/06

ÍNDICE DE CONTENIDO

ACRÓNIMOS

CA - *Certificate Authority* o *Certification Authority.* Entidad de Certificación

CPS - *Certification Practice Statement*. Declaración de Prácticas de Certificación

CRL - *Certificate Revocation List.* Lista de certificados revocados

CSR - *Certificate Signing Request.* Petición de firma de certificado

DES - *Data Encryption Standard*. Estándar de cifrado de datos

DN - *Distinguished Name.* Nombre distintivo dentro del certificado digital

DSA - *Digital Signature Algorithm.* Estándar de algoritmo de firma

DSCF - Dispositivo seguro de creación de firma

DSADCF - Dispositivo seguro de almacén de datos de creación de firma

FIPS - *Federal Information Processing Standard Publication*

IETF - *Internet Engineering Task Force*

ISO - *International Organization for Standardization*. Organismo Internacional de Estandarización

ITU - *International Telecommunications Union.* Unión Internacional de Telecomunicaciones

LDAP - *Lightweight Directory Access Protocol*. Protocolo de acceso a directorios

OCSP - *On-line Certificate Status Protocol.* Protocolo de acceso al estado de los certificados

OID - *Object Identifier*. Identificador de objeto

PA - *Policy Authority.* Autoridad de Políticas

PC - Política de Certificación

PIN - *Personal Identification Number*. Número de identificación personal

PKI - *Public Key Infrastructure*. Infraestructura de clave pública

PSC - Prestador de Servicios de Certificación

RA - *Registration Authority* Autoridad de Registro

RSA - Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado

SHA-1 - *Secure Hash Algorithm.* Algoritmo seguro de Hash

SSL - *Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.

TCP/IP - *Transmission Control Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

DEFINICIONES

Autoridad de Políticas - Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y CPS.

Autoridad de Registro - Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.

Certificación cruzada - El establecimiento de una relación de confianza entre dos CA's, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes.

Certificado - Archivo que asocia la clave pública con algunos datos identificativos del Firmante/Suscriptor y es firmada por la CA.

Clave pública - Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada datos de verificación de firma.

Clave privada - Valor matemático conocido únicamente por el Firmante / Suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada datos de creación de firma.

La clave privada de la CA será usada para firma de certificados y firma de CRL's

CPS - Conjunto de prácticas adoptadas por una Entidad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.

CRL - Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la CA.

Datos de Activación - Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada

DSADCF - *Dispositivo seguro de almacén de los datos de creación de firma.* Elemento software o hardware empleado para custodiar la clave privada del Firmante/Suscriptor de forma que solo él tenga el control sobre la misma.

DSCF - *Dispositivo Seguro de creación de firma*. Elemento software o hardware empleado por el Firmante/Suscriptor para la generación de firmas digitales, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el Firmante/Suscriptor.

Entidad de Certificación - También conocida como Autoridad de Certificación 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, vinculando una determinada clave pública con una persona,

Institución - Dentro del contexto de estas políticas de certificación, aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el Firmante/Suscriptor.

Firma digital - El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera:

a) que los datos no han sido modificados (integridad)
b) que la persona que firma los datos es quien dice ser (identificación)
c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)

OID - Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.

Par de claves - Conjunto formado por la clave pública y privada, ambas relacionadas entre si matemáticamente.

PKI - Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.

Política de Certificación - Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes.

Prestador de Servicios de Certificación - entidad que presta los servicios concretos relativos al ciclo de vida de los certificados.

Firmante/Suscriptor - Dentro del contexto de esta política de certificación, persona cuya clave pública es certificada por la CA y dispone de una privada válida para generar firmas digitales.

S**olicitante -** Persona física que solicita el certificado, y que en el contexto de esta Política coincide con la figura del Firmante/Suscriptor.

Tercero que confía - Dentro del contexto de esta política de certificación, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado

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 de persona física con vínculo institucional, varios subtipos de certificados en función 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 CA de AVANSI C. por A.:

NOMBRE ABREVIADO	**OID**				**DESCRIPCIÓN COMPLETA**
	CA	**TITULAR**	**SOPORTE**	**GENERACIÓN**	
AVS-PF-SW-PSC	2	1	1	1	Certificado de Persona Física con Vínculo Institucional claves almacenadas en software y generadas por el PSC
AVS-PF-SW-USU	2	1	1	2	Certificado de Persona Física con Vínculo Institucional, claves almacenadas en software y generadas por el titular
AVS-PF-HW-PSC	2	1	2	1	Certificado de Persona Física con Vínculo Institucional, claves almacenadas en hardware y generadas por el PSC
AVS-PF-HW-USU	2	1	2	2	Certificado de Persona Física con Vínculo Institucional, claves almacenadas en hardware y generadas por el titular

Esta política en concreto da respuesta a estos 4 subtipos de certificados

1. INTRODUCCIÓN

1.1 CONSIDERACIÓN INICIAL

Por no haber una definición taxativa de los conceptos de Declaración de Prácticas de Certificación y Políticas de Certificación y debido a algunas confusiones formadas, entendemos que es necesario establecer sus diferencias en base a las siguientes definiciones:

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 Prácticas de Certificación** es definida como un conjunto de prácticas adoptadas por una Entidad de Certificación (CA) 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 Entidad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

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

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

En definitiva una política define "**qué"** requerimientos de seguridad son necesarios para la emisión de los certificados. La CPS nos dice "**cómo**" se cumplen los requerimientos de seguridad impuestos por la política.

1.2 GENERALIDADES

El presente documento especifica la Política de Certificación del CERTIFICADO DE PERSONA FÍSICA CON VÍNCULO INSTITUCIONAL, y está basada en la especificación del estándar RCF 2527 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, de IETF y del ETSI TS 101 456 V1.2.1.

Esta Política de Certificación está en conformidad con las disposiciones legales que rigen el tema de Firma Digital en la República Dominicana, en especial en lo que establece la Ley No.126-02, su Reglamento de Aplicación (Dec. No. 335-03) y sus normas complementarias, cumpliendo todos los requisitos técnicos y de seguridad exigidos para la emisión de certificados reconocidos.

Esta política define las reglas y responsabilidades que deben seguir aquellas Entidades de Certificación que deseen emitir el tipo de certificado definido en el presente documento, imponiendo además ciertas obligaciones que deben ser tenidas 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 CA que emita este tipo de certificados, se ajustará a los niveles de seguridad que se detallan en esta política de certificación e informarán a sus Firmantes/Suscriptores de su existencia.

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

La CA suspenderá y revocará sus certificados según lo dispuesto en esta política.

La CA conservará los registros e incidencias de acuerdo con lo que se establece en esta política.

Las funciones críticas del servicio se realizarán al menos por dos personas.

Las claves de los Firmantes/Suscriptores tienen un periodo de validez determinado por esta política y en ningún caso podrán realizarse copias de *backup*, ni almacenarse por la CA.

La información personal recabada del Firmante/Suscriptor se recogerá con el debido consentimiento del interesado y únicamente para los fines propios del servicio de certificación, el cual podrá ejercitar en todo caso sus oportunos derechos de información, rectificación y cancelación. La CA respetará así mismo la normativa aplicable en materia de protección de datos.

Los datos de vinculación de la persona física con la institución pueden no tener ningún efecto en algunos procesos.

La actividad de la CA podrá ser sometida a la inspección de la Autoridad de Políticas (PA) 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. En la página web de AVANSI (www.avansi.com.do) hay algunas informaciones útiles.

1.3 IDENTIFICACIÓN

La presente Política de Certificación está identificada con el OID:

1.3.6.1.4.1.27395.6.2.1

iso (1)
org (3)
dod (6)
internet (1)
private (4)
enterprise (1)
AVANSI C. por A. (27395)
Políticas de certificación (6)
CA AVANSI Certificados Digitales (2)
Persona Física con Vínculo Institucional (1)

1.4 COMUNIDAD Y ÁMBITO DE APLICACIÓN

1.4.1 Entidad de Certificación (CA)

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 (Firmante/Suscriptor) relacionada a una institución concreta, a través de la emisión de un Certificado.

El emisor de este tipo de certificados es AVANSI C. por A. a través de su CA AVANSI Certificados Digitales.

1.4.2 Autoridad de Registro (RA)

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

1.4.3 Firmante ó Suscriptor

Bajo esta Política el Firmante ó Suscriptor es una persona física, vinculada a una determinada institución, poseedor de un dispositivo de creación de firma con un Certificado emitido bajo esta política.

1.4.4 Tercero que confía

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

1.4.5 Solicitante

Se entenderá por Solicitante la persona física que solicita el Certificado. A efectos de esta Política, la figura del Solicitante coincide con la figura del Firmante/Suscriptor.

1.4.6 Institución

A efectos de las presentes políticas de Certificación nos referiremos a una Institución como aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el Firmante/Suscriptor, incluyendo a los empresarios individuales.

La Institución solicitará la suspensión / revocación del certificado cuando cese la vinculación del Firmante/Suscriptor con la organización.

1.4.7 Ámbito de Aplicación y Usos

El Certificado emitido bajo la presente Política, permite identificar a una persona física vinculada a una institución en el ámbito de su actividad. Estos Certificados no son válidos para asumir responsabilidades, compromisos o derechos en nombre de la institución que figura en el Certificado, salvo que por la propia naturaleza del mismo se infiera lo contrario (p. ej. Empresario individual).

El Certificado emitido bajo esta Política puede ser utilizado con los siguientes propósitos:

Identificación del Firmante/Suscriptor y su vinculación con la institución: El Firmante / Suscriptor del Certificado puede autenticar, frente a otra parte, su identidad y su vinculación a la institución, 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 de este Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Firmante/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 la encriptación de datos, la CA no se responsabiliza por esta actividad, debido a que, por motivos de seguridad, esta Política determina que la CA 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 o el Tercero que confía lo hará, en todo caso, bajo su propia responsabilidad.

1.4.7.1 Usos Prohibidos y no Autorizados

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

El empleo de los certificados que implique la realización de operaciones no autorizadas según las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los Contratos de la CA con sus Firmantes/Suscriptores tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la CA, 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 CA mediante la emisión de sus certificados, no es posible por parte de la CA 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 CA.

Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la CA emitir valoración alguna sobre dicho contenido, asumiendo por tanto el signatario cualquier responsabilidad dimanante del contenido de dicho mensaje aparejado al uso de un certificado emitido por la CA. Asimismo, le será imputable al signatario cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los contratos de la CA con sus Firmantes/Suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.5 CONTACTO

La presente política de certificación, está administrada y gestionada por la Gerencia de AVANSI C. por A., pudiendo ser contactado por los siguientes medios:

E-mail:	info@avansi.com.do
Teléfono:	+1 (809) 563 4941
Fax:	+1 (809) 563 6390
Dirección:	AVANSI, C. por A. Mustafa Kemal Ataturk, No. 34, Edificio NPII Tercera planta, 3SO, Ensanche Naco Santo Domingo, DN República Dominicana o AVANSI, C. por A. Apartado Postal 3179 Santo Domingo, DN República Dominicana

2. CLÁUSULAS GENERALES

2.1 OBLIGACIONES

2.1.1 CA

La Entidad Certificadora AVANSI C. por A. actuando bajo esta Política de Certificación está obligada a cumplir con lo dispuesto por la normativa vigente y además a:

a) Respetar lo dispuesto en esta Política.
b) Proteger sus claves privadas de forma segura.
c) Emitir certificados conforme a esta Política y a los estándares de aplicación.
d) Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
e) Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados cualificados.
f) Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
g) Suspender y revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL.
h) Informar a los Firmantes/Suscriptores de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.
i) Publicar esta Política y las Prácticas correspondientes en su página web.
j) Informar sobre las modificaciones de esta Política y de su Declaración Prácticas de Certificación a los suscriptores y RA's que estén vinculadas a ella.
k) No almacenar ni copiar los datos de creación de firma del Firmante/Suscriptor.
l) Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.
m) Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación.
n) Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

2.1.2 RA

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

a) Respetar lo dispuesto en esta Política.
b) Proteger sus claves privadas.
c) Comprobar la identidad de los solicitantes de certificados.
d) Verificar la exactitud y autenticidad de la información suministrada por el Firmante/Suscriptor solicitante.
e) Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Firmante/Suscriptor.
f) Respetar lo dispuesto en los contratos firmados con la CA y con el Firmante/Suscriptor.
g) Informar a la CA las causas de revocación, siempre y cuando tomen conocimiento.

2.1.3 Solicitante

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

a) Suministrar a la RA la información necesaria para realizar una correcta identificación.
b) Confirmar la exactitud y veracidad de la información suministrada.
c) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

2.1.4 Firmante/Suscriptor

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

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

2.1.5 Terceros que confían

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

a) Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
b) 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.

2.1.6 Institución

Será obligación de la Institución solicitar a la RA la suspensión/revocación del certificado cuando cese la vinculación del Firmante/Suscriptor con la organización.

2.1.7 Repositorio

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

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

2.2 RESPONSABILIDAD

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

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

Las responsabilidades de la CA incluyen las establecidas por la presente Política de Certificación, así como las que resulten de aplicación como consecuencia de la normativa dominicana e internacional.

La CA 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:

a) La exactitud de toda la información contenida en el certificado en la fecha de su emisión.
b) 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.
c) La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
d) La correspondencia entre el certificado solicitado y el certificado entregado.
e) Cualquier responsabilidad que se establezca por la legislación vigente.

2.2.1 Exoneración de responsabilidad

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

a) Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
b) Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Certificación.
c) Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Entidad de Certificación.
d) Por el uso de la información contenida en el Certificado o en la CRL.
e) 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.
f) Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
g) Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
h) Por la no recuperación de documentos cifrados con la clave pública del Firmante/Suscriptor.
i) Fraude en la documentación presentada por el solicitante.

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones

Independientemente del importe de las transacciones, este tipo de certificados tienen un límite de responsabilidad igual a ochenta mil dólares de los Estados Unidos de América (USA$ 80,000.00), o su equivalente en moneda de la República Dominicana. Para los casos no previstos por la ley, deberán establecerse garantías particulares a través de seguros específicos que se negociarán individualmente.

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

2.3 RESPONSABILIDAD FINANCIERA

La CA no asume ningún tipo de responsabilidad financiera, salvo lo dispuesto en la legislación vigente.

2.4 INTERPRETACIÓN Y EJECUCIÓN

2.4.1 Legislación

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por lo dispuesto en la legislación dominicana vigente.

2.4.2 Independencia

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

2.4.3 Notificación

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

2.4.4 Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, en base a los procedimientos recogidos en el Reglamento de Solución de Controversias asociado a la Ley 126-02.

2.5 TARIFAS

2.5.1 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 página web de AVANSI C. por A. www.avansi.com.do y/o en la de cada RA concreta.

2.5.2 Tarifas de acceso a los certificados

LA CA no provee en este momento acceso a los certificados emitidos, sólo al listado de certificados revocados (CRL), ver epígrafe siguiente.

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

La CA proveerá de un acceso para verificar la información relativa al estado de un certificado emitido o a la lista de certificados revocados (CRL) de forma gratuita, la CA se reserva el derecho de imponer alguna tarifa para los casos de descarga masiva de CRLs o cualquier otra circunstancia que a juicio de la CA deba ser gravada.

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

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

2.5.5 Política de reintegros

La CA dispondrá de una política de reintegros puesta a disposición de los terceros que confían en la dirección de Internet http://www.avansi.com.do y/o en la de cada RA concreta.

2.6 PUBLICACIÓN Y REPOSITORIOS

2.6.1 Publicación de información de la CA

2.6.1.1 Políticas y Prácticas de Certificación

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

La presente Política de Certificación es pública y se encuentra disponible en el sitio de Internet.

Las Prácticas de Certificación de referencia serán así mismo públicas y se pondrán a disposición del público en la dirección de Internet http://politicas.avansi.com.do

2.6.1.2 Términos y condiciones

La CA o la RA 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 PINES o claves que permitan el acceso a la clave privada.

2.6.1.3 Difusión de los certificados

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados necesarios para los Firmantes/Suscriptores y Terceros que confían son accesibles.

En concreto:

a) El certificado de la CA es público y se encontrará disponible en la página web de AVANSI C. por A. www.avansi.com.do.
b) El listado de certificados revocados (CRL) de la CA es público, salvo lo establecido en el epígrafe 2.5.3.
c) La CA pondrá a disposición de los Terceros que confían los términos y condiciones referentes al uso de los certificados.
d) La información a la que se refieren los 2 primeros puntos estará disponible 24 horas al día, 7 días por semana. En caso de fallo del sistema u otros factores que no se

encuentran bajo el control de la CA, la CA hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

2.6.2 Frecuencia de publicación

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

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

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

2.6.3 Controles de acceso

El acceso a la información será gratuito y estará a disposición de los Firmantes/Suscriptores y terceros que confían, no obstante, y como ya se ha dicho anteriormente la CA se reserva el derecho de imponer alguna tarifa para algún tipo de información que a juicio de la CA deba ser gravada.

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

2.7 AUDITORIAS

Sin perjuicio de la realización de auditorías internas periódicas por parte de las CA, esta se somete a todas las auditorías externas que sean aplicables conforme lo dicta la norma complementaría sobre auditoría aprobada por la autoridad reguladora INDOTEL.

2.8 CONFIDENCIALIDAD

2.8.1 Tipo de información a mantener confidencial

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

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

2.8.2 Tipo de información considerada no confidencial

Se considerará como información no confidencial:

a) La contenida en la presente Política y en las Prácticas de Certificación.
b) La información contenida en los certificados siempre que el Firmante/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.

2.8.3 Divulgación de información de revocación / suspensión de certificados

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

2.8.4 Envío de información a la Autoridad Competente

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

2.9 DERECHOS DE PROPIEDAD INTELECTUAL

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

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 REGISTRO INICIAL

3.1.1 Tipos de nombres

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

3.1.2 Pseudónimos

Los pseudónimos no serán admitidos.

3.1.3 Reglas utilizadas para interpretar varios formatos de nombres

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

3.1.4 Unicidad de los nombres

La CA realizará 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 CA es responsable de realizar los esfuerzos que razonablemente estén a su alcance para asegurar que el Número de Serie es suficiente para resolver las posibles colisiones entre nombres.

3.1.5 Procedimiento de resolución de disputas de nombres

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

3.1.6 Reconocimiento, autenticación y función de las marcas registradas

Se admitirá la identificación de marcas o acrónimos de entidades siempre que en el propio certificado aparezca, además, la razón social de la institución u otro elemento de identificación inequívoco, como número del Registro Nacional de Contribuyente.

3.1.7 Métodos de prueba de la posesión de la clave privada

Si el par de claves es generado por el Firmante/Suscriptor, la CA proveerá en la CPS la garantía de estar en posesión de clave privada. En caso contrario, la CA tomará las medidas necesarias que aseguren que el Firmante/Suscriptor está en posesión de la clave privada asociada a la clave pública.

3.1.8 Autenticación de la identidad de una organización

Los Certificados emitidos bajo la presente Política identifican a una persona física vinculada a una institución, por lo que se exigirá, en todo caso, la acreditación de la existencia de la institución por un medio conforme a Derecho.

El Certificado no otorga ninguna capacidad de representación, únicamente refleja algún tipo de vínculo entre la persona física y la institución.

3.1.9 Autenticación de la identidad de un individuo

Para realizar una correcta identificación de la identidad del solicitante, se atenderá a lo dispuesto por la legislación vigente.

Para la mencionada comprobación de la identidad del solicitante se exigirá la presencia física del mismo.

3.1.10 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.

La RA únicamente comprobará la documentación que en su caso presente el Firmante/Suscriptor respecto de los datos cuya modificación ha declarado.

3.1.11 Requerimientos aplicables a las RA's externas

Cuando la CA emplee RA's externas asegurará los siguientes aspectos:

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

3.2 RENOVACIÓN DE LA CLAVE Y DEL CERTIFICADO

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

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

Un certificado podrá ser renovado un máximo de tres veces, debiendo proceder a una nueva solicitud una vez transcurrido este plazo siguiendo el procedimiento empleado para una primera solicitud.

La personación física del solicitante 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 personación física siempre que hayan transcurrido más de 5 años desde la última verificación de la identidad realizada mediante la personación física del solicitante.

3.3 REEMISIÓN DESPUÉS DE UNA REVOCACIÓN

La CA no realizará reemisiones.

3.4 SOLICITUD DE REVOCACIÓN

Todas las solicitudes de revocación serán autenticadas.

4. REQUERIMIENTOS OPERACIONALES

4.1 SOLICITUD DE CERTIFICADOS

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

4.1.1 Registro

a) Antes de comenzar una relación contractual, la CA, por sí misma o por medio de la RA, informará al Firmante/Suscriptor de los términos y condiciones relativos al uso del certificado.

b) Se comunicará esta información a través de un medio de comunicación perdurable, susceptible de ser transmitido electrónicamente y en un lenguaje comprensible.

c) La CA, por sí misma o por medio de la RA, comprobará, de acuerdo con la legislación vigente, la identidad y los atributos específicos del Firmante/Suscriptor. La comprobación de la identidad se realizará mediante la personación física del Firmante/Suscriptor y la exhibición por éste de la Cédula de Identidad y Electoral o el Pasaporte.

d) Se registrará en todo caso:

1) Nombre completo del Firmante/Suscriptor tal y como aparece en el documento de identificación presentado.
2) Fecha y lugar de nacimiento, número de la Cédula de Identidad y Electoral o del Pasaporte.
3) Nombre completo y forma jurídica de la institución a la que se vincula el firmante/Suscriptor.
4) Evidencia de la existencia de la institución.
5) Evidencia de la vinculación existente entre el Firmante/Suscriptor y la institución.

e) El Firmante/Suscriptor facilitará su dirección física u otros datos que permitan contactar con él.

f) La CA registrará 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.

g) La CA guardará el contrato firmado con el Firmante/Suscriptor, el cual incluirá:

1) Acuerdo de las obligaciones del Firmante/Suscriptor.
2) Consentimiento para que la CA guarde la información usada para el registro, así como para el traspaso de información a una tercera parte en el caso de que la CA cese su actividad.
3) Si y bajo que condiciones el Firmante/Suscriptor consiente la publicación de su certificado
4) Que la información contenida en el certificado es correcta

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

i) Si el par de claves no es generado por la CA, ésta realizará 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.

j) La CA cumplirá con todos los requisitos impuestos por la legislación aplicable en materia de protección de datos.

4.2 EMISIÓN DE CERTIFICADOS

La CA pondrá todos los medios a su alcance para asegurar que la emisión y renovación de certificados se realice de una forma segura. En particular:

a) Cuando la CA genere las claves del Firmante/Suscriptor, que el procedimiento de emisión del certificado está ligado de manera segura a la generación del par de claves por la CA.
b) Cuando la CA no genere las claves del Firmante/Suscriptor, que la clave privada o el dispositivo seguro de creación de firma ha sido generado de manera segura por el Firmante/Suscriptor.
c) La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los DN asignados a los Firmantes/Suscriptores.

d) 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.
e) La CA verificará que el registro de los datos es intercambiado con proveedores de servicios reconocidos, cuya identidad es autenticada.
f) La CA notificará al solicitante de la emisión de su certificado.

4.3 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 se realizará de forma expresa, por escrito y ante el encargado de la CA o RA. El solicitante emitirá esta aceptación en su propio nombre y, en su caso, en nombre y representación de la institución que vaya a ser vinculada por el propio certificado.

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 CA y el contenido del certificado, se comunicará de inmediato a la CA para que proceda a su revocación y a la emisión de un nuevo certificado. La CA 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 RA, la CA o cualquier tercero que de buena fe confíe en el contenido del Certificado.

4.4 SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS

4.4.1 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.

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

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

4.4.2 Causas de revocación

Los Certificados se revocarán cuando concurra alguna de las circunstancias siguientes:

a) Solicitud voluntaria del Firmante/Suscriptor.
b) Pérdida o inutilización por daños del soporte del certificado.
c) Fallecimiento del Firmante/Suscriptor o incapacidad sobrevenida, total o parcial.
d) Terminación de la vinculación con la institución.
e) Cese en la actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
f) Inexactitudes graves en los datos aportados por el signatario 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.
g) Que se detecte que las claves privadas del Firmante/Suscriptor o de la CA 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.
h) Por incumplimiento por parte de la RA, CA o el Firmante/Suscriptor de las obligaciones establecidas en esta política.
i) Por la resolución del contrato con el Firmante/Suscriptor.
j) 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.
k) Por resolución judicial o administrativa que lo ordene.
l) Por la extinción de la institución.
m) Por la concurrencia de cualquier otra causa especificada en la presente política.

4.4.3 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse únicamente por el Firmante/Suscriptor, un representante de la institución a la que pertenece o por la propia CA.

Todas las solicitudes serán en todo caso autenticadas.

4.4.4 Procedimiento de solicitud de revocación

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

La información relativa al retraso máximo entre la recepción de una petición de revocación y su paso al estado de suspendido estará disponible para todos los terceros que confían. Este será como máximo de 3 horas.

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

El Firmante/Suscriptor cuyo certificado haya sido suspendido o revocado será informado del cambio de estado de su certificado. Así mismo, el Firmante/Suscriptor será informado del levantamiento de la suspensión. La CA utilizará todos los medios a su alcance para conseguir este objetivo, pudiendo intentar la mencionada comunicación por e-mail, teléfono, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

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

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

La CRL, en su caso, será firmada por la CA.

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 CA, la CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

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

Se realizarán 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 estará disponible públicamente.

4.4.5 Periodo de revocación

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

4.4.6 Suspensión

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

4.4.7 Procedimiento para la solicitud de suspensión

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

4.4.8 Límites del periodo de suspensión

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

4.4.9 Frecuencia de emisión de CRL's

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

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

4.4.10 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. No obstante la CA podrá imponer una tarifa por el acceso a la CRL.

4.4.11 Disponibilidad de comprobación *on-line* de la revocación

Se proporcionará un servicio *on-line* de comprobación de revocaciones, el cual estará disponible las 24 horas del día los 7 días de la semana. En caso de fallo del sistema, del servicio o de cualquier otro factor que no esté bajo el control de la CA, la CA realizará 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.

4.4.12 Requisitos de la comprobación de la revocación

El tercero que confía que desee comprobar la revocación de un certificado, podrá hacerlo consultando las CRLs a través de la página web de la CA www.avansi.com.do de forma gratuita.

No obstante lo anterior, el acceso a este sistema de consulta de certificados podrá restringirse según lo establecido en el epígrafe 4.4.10.

4.4.13 Otras formas de divulgación de información de revocación disponibles

No estipulado.

4.4.14 Requisitos de comprobación para otras formas de divulgación de información de revocación

No estipulado.

4.4.15 Requisitos especiales de revocación por compromiso de las claves

No estipulado.

4.5 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

La CA realizará 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:

General

a) Se realizarán 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 serán almacenados, completa y confidencialmente, de acuerdo con las prácticas de negocio.

c) Los registros relativos a los certificados estarán disponibles si estos son requeridos a efectos probatorios en los procedimientos legales.

d) Será almacenado el momento exacto en que se produzcan los eventos relativos a la gestión de las claves y la gestión de los certificados.

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 digitales.

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 CA.

Registro

h) La CA realizará 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.

i) La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relativa al registro es almacenada, incluyendo la siguiente:

1) La documentación presentada por el solicitante para el registro.
2) Número de la Cédula de Identidad y Electoral, del Pasaporte o de cualquier otro documento acreditativo de la identidad del solicitante.
3) Copia de documentos identificativos (cédula, pasaporte,...), incluido el contrato suscrito con el Firmante/Suscriptor.
4) Algunas cláusulas específicas contenidas en el contrato (p.ej. el consentimiento de la publicación del certificado).
5) Método empleado para comprobar la validez de los documentos identificativos, si existe.
6) Nombre de la Autoridad de Registro.

j) La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar la privacidad de la información relativa al Firmante/Suscriptor.

Generación del certificado

k) La CA registrará todos los eventos relativos al ciclo de vida de las claves de la CA.

l) La CA registrará todos los eventos relativos al ciclo de vida de los certificados.

Entrega del dispositivo al Firmante/Suscriptor

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

Gestión de la revocación

n) La CA realizará 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.

4.5.1 Tipos de eventos registrados

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

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

a) encendido y apagado del sistema.
b) encendido y apagado de la aplicación de la CA.
c) intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
d) cambios en los detalles de la CA y/o sus claves.
e) cambios en la creación de políticas de certificados.
f) intentos de inicio y fin de sesión.
g) intentos de accesos no autorizados al sistema de la CA a través de la red.
h) intentos de accesos no autorizados al sistema de archivos.
i) generación de claves propias.
j) creación y revocación de certificados.
k) intentos de dar de alta, eliminar, habilitar y deshabilitar Firmantes/Suscriptores y actualizar.
l) acceso físico a los *logs.*
m) cambios en la configuración y mantenimiento del sistema.
n) cambios personales.
o) registros de la destrucción de los medios que contienen las claves, datos de activación.

4.5.2 Frecuencia de procesado de Logs

La CA revisará sus *logs* periódicamente y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente.

La CA se asegurará así mismo de que los *logs* no han sido manipulados y documentará las acciones tomadas ante esta revisión.

4.5.3 Periodos de retención para los Logs de auditoria

La información almacenada se conservará al menos durante 5 años.

4.5.4 Protección de los Logs de auditoría

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

4.5.5 Procedimientos de backup de los Logs de auditoría

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

4.5.6 Sistema de recogida de información de auditoria

No estipulado.

4.5.7 Notificación al sujeto causa del evento

No estipulado.

4.5.8 Análisis de vulnerabilidades

Se realizará 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.

4.6 ARCHIVO DE REGISTROS

4.6.1 Tipo de archivos registrados

Los siguientes datos y archivos deben ser almacenados por la CA o por delegación de ésta.

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

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

4.6.2 Periodo de retención para el archivo

La información detallada en el apartado 4.5 i), k) y l), los contratos con los Firmantes/Suscriptores y cualquier información relativa a la identificación y autenticación del Firmante/Suscriptor se conservará durante al menos 20 años.

4.6.3 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.

4.6.4 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*.

4.6.5 Requerimientos para el sellado de tiempo de los registros

No estipulado.

4.6.6 Sistema de recogida de información de auditoria

No estipulado.

4.6.7 Procedimientos para obtener y verificar información archivada

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

Este procedimiento regulará 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.

4.7 CAMBIO DE CLAVE DE LA CA

Antes de que el uso de la clave privada de la CA caduque se realizará un cambio de claves. La vieja CA y su clave privada se desactivarán y se generará una nueva CA con una clave privada nueva y un nuevo DN.

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

a) Clave pública de la nueva CA firmada por la clave privada de la vieja CA.
b) Clave pública de la vieja CA firmada con la clave privada de la nueva CA.

4.8 RECUPERACIÓN EN CASO DE COMPROMISO DE LA CLAVE O DESASTRE

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar, en caso de desastre o compromiso de la clave privada de la CA, que ésta será restablecida tan pronto como sea posible.

4.8.1 La clave de la CA se compromete

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

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

a) Informar a todos los Firmantes/Suscriptores, terceros que confían y otras CAs con los cuales tenga acuerdos u otro tipo de relación del compromiso.
b) Indicar que los certificados e información relativa al estado de la revocación firmados usando esta clave pueden no ser válidos.

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

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

La CA 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.

4.9 CESE DE LA CA

La CA realizará 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 realizará, como mínimo, las siguientes actuaciones:

1) Informar a todos los Firmantes/Suscriptores, terceros que confían y otras CAs con los cuales tenga acuerdos u otro tipo de relación del cese.
2) La CA revocará toda autorización a entidades subcontratadas para actuar en nombre de la CA en el procedimiento de emisión de certificados.
3) La CA 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.
4) Las claves privadas de la CA serán destruidas y deshabilitadas para su uso.

b) La CA 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 CPS las previsiones hechas para el caso de cese de actividad. Estas incluirán:

1) informar a las entidades afectadas.
2) transferencia de las obligaciones de la CA a otras partes.

3) cómo debe ser tratada la revocación de certificados emitidos cuyo periodo de validez aun no ha expirado.
4) En particular, la CA:
   a) informará puntualmente a todos los Firmantes/Suscriptores, empleados, terceros que confían y RAs con una anticipación mínima de 3 meses antes del cese.
   b) transferirá todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación.

5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL

5.1 CONTROLES DE SEGURIDAD FÍSICA

La CA realizará 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:

CA 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 será limitado a las personas autorizadas y las instalaciones en las que se firman los certificados estarán protegidas de las amenazas físicas.

b) Se establecerán controles para impedir la perdida, daño o compromiso de los activos de la empresa y la interrupción de la actividad.

c) Se establecerán controles para evitar el compromiso o robo de información.

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

d) Las actividades relativas a la generación de certificados y gestión de revocaciones serán realizadas en un espacio protegido físicamente de accesos no autorizados al sistema o a los datos.

e) La protección física se conseguirá por medio de la creación de unos anillos de seguridad claramente definidos (p.ej. barreras físicas) alrededor de la generación de certificados y gestión de revocaciones. Aquellas partes de esta tarea compartidas con otras organizaciones quedarán fuera de este perímetro.

f) Los controles de seguridad física y medioambiental serán implementados para proteger las instalaciones que albergan los recursos del sistema, los recursos del sistema en si mismos y

las instalaciones usadas para soportar sus operaciones. Los programas de seguridad física y medioambiental de la CA 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, etc.

g) Se implementarán controles para evitar que los equipos, la información, soportes y software relativos a los servicios de la CA sean sacados de las instalaciones sin autorización.

5.1.1 Ubicación y construcción

Las instalaciones de la CA deben estar 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.

5.1.2 Acceso físico

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

5.1.3 Alimentación eléctrica y aire acondicionado

La CA realizará 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 CA.

5.1.4 Exposición al agua

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

5.1.5 Protección y prevención de incendios

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

5.1.6 Sistema de almacenamiento.

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

5.1.7 Eliminación de residuos

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

5.1.8 Backup remoto

La CA realizará 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.

5.2 CONTROLES PROCEDIMENTALES

5.2.1 Roles de confianza

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

Los roles de confianza incluyen las siguientes responsabilidades:

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

Administradores de sistema: Están autorizados para instalar, configurar y mantener los sistemas y aplicaciones de confianza de la CA que soportan las operaciones de Certificación.

Operador de sistema: Está autorizado para realizar funciones relacionadas con el sistema de *backup* y de recuperación.

Administrador de CA: Responsable de la Administración y control de gestión de los sistemas de confianza de la CA.

Operador de CA: Realizan funciones de apoyo en el control dual de las operaciones de la CA.

Auditor de CA: Realiza las labores de supervisión y control de la implementación de las políticas de seguridad.

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

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

5.2.2 Número de personas requeridas por tarea

Las siguientes tareas requerirán al menos un control dual:

a) La generación de la clave de la CA.
b) La recuperación y back-up de la clave privada de la CA.
c) Activación de la clave privada de la CA.
d) Cualquier actividad realizada sobre los recursos HW y SW que dan soporte a la entidad de certificación.

5.2.3 Identificación y autentificación para cada rol

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

5.3 CONTROLES DE SEGURIDAD DE PERSONAL

5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

La CA realizará 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:

CA General

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

c) Se describirá el trabajo del personal de la CA (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 CA.

d) El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.

Registro, generación de certificados y gestión de revocaciones

e) Se empleará el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de firma digital y esté familiarizado con procedimientos de seguridad.

f) Todo el personal implicado en roles de confianza estará libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de la CA.

g) El personal de la CA será formalmente designado para desempeñar roles de confianza por el responsable de seguridad.

h) La CA 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.

5.3.2 Procedimientos de comprobación de antecedentes

La CA 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 CA que propicie la confianza suficiente en el empleado. Se entenderá como experiencia necesaria el haber pertenecido al Departamento en cuestión durante al menos 6 meses.

5.3.3 Requerimientos de formación

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

a) los principales mecanismos de seguridad de CA y/o RA.
b) todo el software de PKI y sus versiones empleados en el sistema de la CA.
c) todas las tareas de PKI que se espera que realicen.
d) los procedimientos de resolución de contingencias y continuidad de negocio.

5.3.4 Requerimientos y frecuencia de la actualización de la formación

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

5.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado.

5.3.6 Sanciones por acciones no autorizadas

La CA fijará las posibles sanciones por la realización de acciones no autorizadas.

5.3.7 Requerimientos de contratación de personal

Ver el apartado 5.3.1.

5.3.8 Documentación proporcionada al personal

Todo el personal de la CA y RA recibirán los manuales de usuario en los que se detallen al menos los procedimientos para el registro de certificados, creación, actualización, renovación, suspensión, revocación y la funcionalidad del software empleado.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 Generación del par de claves de la CA

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

En particular:

a) La generación de la clave de la CA 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 CPS.

b) La generación de la clave de la CA se realizará en un dispositivo que cumpla los requerimientos que se detallan en el FIPS 140-1, en su nivel 2 o superior.

6.1.2 Generación del par de claves del Firmante/Suscriptor

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

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

a) Las claves serán generadas usando un algoritmo adecuado para los propósitos de la firma digital.

b) Las claves tendrán una longitud de clave adecuada para los propósitos de la firma digital y para el algoritmo de clave pública empleada.

c) Las claves serán generadas y guardadas de forma segura antes de entregárselas al Firmante/Suscriptor.

d) Las claves serán destruidas de forma segura después de su entrega al Firmante/Suscriptor.

6.1.3 Entrega de la clave privada al Firmante/Suscriptor

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

La clave privada será 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 CA entrega un dispositivo seguro al Firmante/Suscriptor, lo hará de forma segura. En particular:

a) La preparación del dispositivo seguro, será 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 usuario (p.ej. un código PIN), los datos de activación se prepararán de forma segura y se distribuirán de manera separada del dispositivo seguro de creación de firma.

6.1.4 Entrega de la clave pública del Firmante/Suscriptor al emisor del certificado

Cuando el Firmante/Suscriptor pueda generar sus propias claves, la clave pública del Firmante/Suscriptor tiene que ser transferida a la RA o CA, de forma que se asegure que,

a) no ha sido cambiado durante el traslado
b) el remitente está en posesión de la clave privada que se corresponde con la clave pública transferida y
c) el proveedor de la clave pública es el legítimo usuario que aparece en el certificado

6.1.5 Entrega de la clave pública de la CA a los Terceros que confían

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que la integridad y la autenticidad de la clave pública de la CA y los parámetros a ella asociados son mantenidos durante su distribución a los terceros que confían. En particular:

a) La clave pública de la CA 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 CA y su *fingerprint* (huella digital) estarán a disposición de los terceros que confían a través de su página web.

6.1.6 Tamaño y periodo de validez de las claves del emisor

El emisor usará claves basadas en el algoritmo RSA con una longitud mínima de 1024 bits para firmar certificados.

El periodo de uso de una clave privada será como máximo de 40 años, después del cual se cambiarán estas claves.

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

a) El periodo de uso de la clave privada de la CA, y
b) El periodo máximo de validez de los certificados de los Firmantes/Suscriptores firmados con esa clave

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

El Firmante/Suscriptor usará claves basadas en el algoritmo RSA con una longitud mínima de 1024 bits.

El periodo de uso de la clave pública y privada del Firmante/Suscriptor no será 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.

6.1.8 Parámetros de generación de la clave pública

No estipulado.

6.1.9 Comprobación de la calidad de los parámetros

No estipulado.

6.1.10 Hardware/software de generación de claves

Las claves de la CA serán generadas en un módulo criptográfico validado al menos por el nivel 2 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

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

6.1.11 Fines del uso de la clave

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

La clave privada del Firmante/Suscriptor será usada únicamente para la generación de firmas digitales, de acuerdo con el apartado 1.4.7.

6.2 PROTECCIÓN DE LA CLAVE PRIVADA

De la CA

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

a) La clave privada de firma de la CA será mantenida y usada en un dispositivo criptográfico seguro, el cual cumple los requerimientos que se detallan en el FIPS 140-1, en su nivel 2 o superior.

b) Cuando la clave privada de la CA esté fuera del módulo criptográfico esta estará cifrada.

c) Se hará un *backup* de la clave privada de firma de la CA, que será 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 CPS.

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

Del Firmante/Suscriptor

La CA realizará 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

6.3 ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 2 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

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

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

6.3.2 Depósito de la clave privada (*key escrow*)

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

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

6.3.3 Copia de seguridad de la clave privada

La CA realizará 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.

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

6.3.4 Archivo de la clave privada

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

Las claves privadas de Firmante/Suscriptor no pueden ser archivadas por la CA.

6.3.5 Introducción de la clave privada en el módulo criptográfico

Ya visto.

6.3.6 Método de activación de la clave privada

La clave privada de la CA será activada conforme al apartado 6.3.1.

Se protegerá 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 se realizará por medio de un canal seguro.

Estos datos de activación tendrán 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.

6.3.7 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.

6.3.8 Método de destrucción de la clave privada

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

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

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

Las claves privadas de los Firmantes/Suscriptores serán destruidas o se harán inservibles después del fin de su ciclo de vida por el propio Firmante/Suscriptor.

6.4 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.4.1 Archivo de la clave pública

La CA conservará todas las claves públicas de verificación.

6.4.2 Periodo de uso para las claves públicas y privadas

Ya visto.

6.5 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 CA, por si misma o por delegación de esta función, realizará los mayores esfuerzos 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 CA 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.

6.6 CONTROLES DE SEGURIDAD INFORMÁTICA

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

a) identificación de todos los terceros que confían
b) controles de acceso basados en privilegios
c) control dual para ciertas operaciones relativas a la seguridad
d) generación de *logs*, revisión de auditoria y archivo de todos los eventos relacionados con la seguridad
e) *backup* y recuperación

6.6.1 Requerimientos técnicos de seguridad informática específicos

Cada servidor de CA incluirá las siguientes funcionalidades:

a) control de acceso a los servicios de CA y gestión de privilegios
b) imposición de separación de tareas para la gestión de privilegios
c) identificación y autenticación de roles asociados a identidades
d) archivo del historial del Firmante/Suscriptor y la CA y datos de auditoria
e) auditoria de eventos relativos a la seguridad
f) auto-diagnóstico de seguridad relacionado con los servicios de la CA
g) mecanismos de recuperación de claves y del sistema de CA

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

6.6.2 Valoración de la seguridad informática

No estipulado.

6.7 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.7.1 Controles de desarrollo del sistema

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

6.7.2 Controles de gestión de la seguridad

6.7.2.1 Gestión de seguridad

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

b) La CA desarrollará 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 CA se mantendrá en todo momento. Cualquier cambio que pueda afectar al nivel de seguridad establecido será aprobado por el foro de gestión de CA.

d) Los controles de seguridad y procedimientos operativos para las instalaciones de la CA, sistemas e información necesarios para los servicios de certificación serán documentados, implementados y mantenidos.

e) La CA realizará 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 CA haya sido subcontratada a otra organización.

6.7.2.2 Clasificación y gestión de información y bienes

La CA realizará 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 CA 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.

6.7.2.3 Operaciones de gestión

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

a) se protegerá la integridad de los sistemas de CA 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 serán minimizados por medio del uso de reportes de incidencias y procedimientos de respuesta.

c) Los soportes serán custodiados de manera segura para protegerlos de daños, robo y accesos no autorizados.

d) Se establecerán e implementarán los procedimientos para todos los roles administrativos y de confianza que afecten a la prestación de servicios de certificación.

Tratamiento de los soportes y seguridad

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

Planning del sistema

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

Reportes de incidencias y respuesta

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

Procedimientos operacionales y responsabilidades

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

6.7.2.4 Gestión del sistema de acceso

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

CA 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 CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar la efectiva administración de acceso de terceros que confían (incluyendo operadores, administradores y cualquier usuario 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 CA realizará 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 CA dispone de los controles de seguridad suficientes para la separación de los roles de confianza identificados en la CPS, 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 CA identificado y autenticado antes de usar aplicaciones críticas relativas a la gestión de certificados.

f) El personal de la CA será responsable de sus actos, por ejemplo, por retener *logs* de eventos.

g) Se protegerán los datos sensibles contra medios de almacenamiento susceptibles de que la información sea recuperada y accesible por personas no autorizadas.

Generación del certificado

h) La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que los componentes de la red local (p. ej. *routers*) están guardados en un medio físico seguro y sus configuraciones son periódicamente auditadas.

i) Las instalaciones de la CA 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.

6.7.2.5 Gestión de la revocación

j) Las instalaciones de la CA 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.

6.7.2.6 Gestión del ciclo de vida del hardware criptográfico

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

a) el hardware criptográfico de firma de certificados no se manipula durante su transporte.

b) el hardware criptográfico de firma de certificados no se manipula mientras está almacenado.

c) el uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

d) el hardware criptográfico de firma de certificados está funcionando correctamente, y

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

6.7.3 Evaluación de la seguridad del ciclo de vida

No estipulado.

6.8 CONTROLES DE SEGURIDAD DE LA RED

Ya definido.

6.9 CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

Todas las operaciones criptográficas de la CA deben ser desarrolladas en un módulo validado por al menos el nivel 2 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

7. PERFILES DE CERTIFICADO Y CRL

7.1 PERFIL DE CERTIFICADO

Todos los certificados emitidos bajo esta política serán conformes al estándar X.509 versión 3 y al RFC 3039 "*Internet X.509 Public Key Infrastructure Qualified Certificates Profile*".

7.1.1 Número de versión

Se indicará en el campo versión que se trata de la v.3

7.1.2 Extensiones del certificado

EXTENSIÓN DEL CERTIFICADO		**VALOR**
Versión		V3
Número de serie		<nº de serie del certificado>
Algoritmo de firma		sha1RSA
Emisor	C	DO
	L	APARTADO POSTAL 3179 SANTO DOMINGO - REPUBLICA DOMINICANA
	O	AVANSI C. POR A. - RNC 130222509
	CN	AVANSI CERTIFICADOS DIGITALES
Válido desde		<fecha de inicio de la validez>
Válido hasta		<fecha de fin de la validez>
Asunto	C	DO
	O	<Nombre institución>
	OU	<Departamento del titular>
	T	<Cargo del titular>
	SN	<Primer apellido>
	G	<Nombre(s)>
	Número de serie	<No. de cédula o pasaporte>
	CN	<Nombre del Firmante/Suscriptor con todos los apellidos>
	Description	Certificado de Persona Física con Vinculo Institucional
Clave pública		RSA (1024 Bits)
Uso mejorado de clave		Autenticación del cliente(1.3.6.1.5.5.7.3.2) Correo seguro(1.3.6.1.5.5.7.3.4)
Identificador de clave de asunto		<Id de clave>
Identificador de clave de entidad emisora		<Id. de clave>=da 6d 93 5f e8 45 62 61 ff d4 aa 7f 88 63 3d 5c d7 0b 4e 51

Nombre alternativo del sujeto	Nombre RFC822=<email titular>
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.27395.6.2.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Texto de aviso=Para información mas detallada sobre las políticas de AVANSI C. POR A. conéctese a http://politicas.avansi.com.do
Punto de distribución CRL	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://crl.avansi.com.do/avansicertificados.crl [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://crl2.avansi.com.do/avansicertificados.crl [3]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://avansicpora.avansi.com/avansicertificados.crl
Restricción básicas	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno
Uso de la clave	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos(f0)
Algoritmo de identificación	sha1
Huella digital	<fingerprint>
Nombre descriptivo	<Nombre y apellidos del solicitante>'s AVANSI C. POR A. – RNC 130222509

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma será 1.2.840.113549.1.1.5

El identificador de objeto del algoritmo de la clave pública será rsaEncryption 1.2.840.113549.1.1.1

7.1.4 Restricciones de los nombres

No estipulado.

7.2 PERFIL DE CRL

Versión	V2
Emisor	C = DO L = APARTADO POSTAL 3179 SANTO DOMINGO - REPUBLICA DOMINICANA O = AVANSI C. POR A. - RNC 130222509 CN = AVANSI CERTIFICADOS DIGITALES
Periodo máximo de validez	1 día
Algoritmo de firma	sha1RSA
Identificador de clave de autoridad	Id. de clave=da 6d 93 5f e8 45 62 61 ff d4 aa 7f 88 63 3d 5c d7 0b 4e 51
URL de distribución	http://crl.avansi.com.do/avansicpora.crl

7.2.1 Número de versión

Se indicará en el campo versión que se trata de la v.2

7.2.2 CRL y extensiones

No estipulado.

8. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

8.1 AUTORIDAD DE LAS POLÍTICAS

La Gerencia de AVANSI C. por A. constituye la autoridad de las políticas (PA) y es responsable de la administración de las políticas.

8.2 PROCEDIMIENTOS DE ESPECIFICACIÓN DE CAMBIOS

Cualquier elemento de esta política es susceptible de ser modificado.

Todos los cambios realizados sobre las políticas serán inmediatamente publicados en la web de AVANSI C. por A.

En la web de AVANSI C. por A. 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.

8.3 PUBLICACIÓN Y COPIA DE LA POLÍTICA

Una copia de esta política estará disponible en formato electrónico en la dirección de Internet: http://politicas.avansi.com.do

8.4 PROCEDIMIENTOS DE APROBACIÓN DE LA CPS

Para la aprobación y autorización de una CA se respetarán los procedimientos especificados por la PA. Las partes de la CPS de una CA que contenga información relevante en relación a su seguridad, toda o parte de esa CPS no estarán disponibles públicamente.