Política de Certificación para CEIF-PJ

Entidades de Intermediación Financiera - Persona Jurídica

ver. 1.1

Título del Documento:	Política de Certificación de CEIF-PJ		
Nombre del documento:	PC-AVS-CEIF-PJ-1.0.pdf		
Versión:	1.1	**Fecha de publicación:**	01 de octubre de 2011
Código:	AVS-PC-CEIF-PJ	**Última revisión:**	01 de octubre de 2011
Estado del documento:	Activo	**Idioma:**	Español
Referencia (OID):	1.3.6.1.4.1.27395.6.2.5	**Núm. Páginas:**	72
Elaborado por:	AVANSI CA		
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 certificado.		
Localización:	http://cps.avansi.com.do		

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	Versión	Motivo del cambio
01-09-2011	1.0	Primera Versión
01-10-2011	1.1	Cantidad de años en la Vigencia

ÍNDICE

I - 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

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

DSCF - Dispositivo seguro 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.

II – DEFINICIONES

Autoridad de Certificación, Entidad de Certificación o CA: 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 sus relaciones electrónicas. El emisor de los de certificados es AVANSI S.R.L. a través de su CA AVANSI Certificados Digitales.

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 - 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 subscriptores del Certificado y aquellas que se dispongan en las Prácticas de Certificación concretas.

Certificación cruzada - 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, el mismo también podrá ser llamado certificado raíz.

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

Documento de identidad: Documento acreditativo con el cual se identifica al Firmante/Subscriptor. Bajo estas políticas dicho documento será Cédula de Identidad, Cédula de Identidad y Electoral o Pasaporte.

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.

EIF – Entidad de Intermediación Financiera.

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)

Firmante o Suscriptor - Persona jurídica poseedora de un dispositivo de creación de firma con un Certificado emitido bajo esta política.

Institución - Persona jurídica que solicita el certificado, y que en el contexto de esta Política, puede coincidir con la figura del Firmante/Suscriptor.

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.

Solicitante - Persona física que solicita el Certificado, responsable de la custodia del mismo. Podrán solicitar el certificado de persona jurídica sus administradores y representantes legales.

Tercero que confía - 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.

III - IDENTIFICADOR 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 jurídica, 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:

NOMBRE ABREVIADO	OID				DESCRIPCIÓN COMPLETA
	CA	TITULAR	SOPORTE	GENERACIÓN	
AVS-CEIF-PJ-SW-PSC	2	1	1	1	CEIF-PJ, claves almacenadas en software y generadas por el PSC
AVS-CEIF-PJ-SW-USU	2	1	1	2	CEIF-PJ, claves almacenadas en software y generadas por el titular
AVS-CEIF-PJ-HW-PSC	2	1	2	1	CEIF-PJ, claves almacenadas en hardware y generadas por el PSC
AVS-CEIF-PJ-HW-USU	2	1	2	2	CEIF-PJ, 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 ENTIDAD DE INTERMEDIACIÓN FINANCIERA - PERSONA JURÍDICA, 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.

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:

1.3.6.1.4.1.27395.6.2.5

ISO (1)	Enterprise (1)
ORG (3)	AVANSI (27395)
DOD (6)	Políticas de certificación (6)
Internet (1)	CA AVANSI Certificados Digitales (2)
Private (4)	CEIF - Persona Jurídica (5)

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 institución o unidad de trabajo (Firmante/Suscriptor) a través de la emisión de un Certificado. El emisor de este tipo de certificados es AVANSI 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 subscriptores del Certificado y aquellas que se dispongan en las Prácticas de Certificación concretas.

1.4.3 - Firmante o Suscriptor

Bajo esta Política el Firmante ó Suscriptor es una persona jurídica, y en concreto, una Entidad de Intermediación Financiera, en adelante EIF, 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, responsable de la custodia del mismo. Podrán solicitar el certificado de persona jurídica sus administradores, representantes legales o aquellas personas físicas debidamente autorizadas mediante documento que acredite las facultades del signatario para actuar en nombre de la persona jurídica, así como las condiciones y límites para su uso.

1.4.6 - Institución

Se entenderá por institución a la persona jurídica que solicita el certificado, y que en el contexto de esta Política, puede coincidir con la figura del Firmante/Suscriptor.

1.4.7 - Ámbito de Aplicación y Usos

Usos Generales

El Certificado emitido bajo la presente Política, permite identificar a una **Entidad de Intermediación Financiera**, como **persona jurídica** en el ámbito descrito principalmente por los sistemas de información que rodean al proyecto de Cámara de Compensación Electrónica de Cheques regulado por el Banco Central de la República. El Certificado emitido bajo esta Política puede ser utilizado con los siguientes propósitos:

a) **Identificar al Firmante/Suscriptor:** El Firmante/Suscriptor podrá identificarse válidamente ante cualquier persona o sistema mediante la firma de un correo electrónico o cualquier otro tipo de datos.

b) **Firma digital de documentos, correos electrónicos y otros documentos digitales:** Por medio de este certificado el Firmante/Suscriptor podrá firmar digitalmente documentos que tendrán validez legal y de esta forma reemplazará la firma manuscrita.

c) **Tramitar con el Estado, Banco Central de la República, otras Entidades de Intermediación Financiera y, en general, con terceros que confían.**

d) **Integridad del documento firmado:** El uso de este Certificado garantiza que el documento o correo electrónico 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

e) **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.

Cámara de Compensación Electrónica de Cheques

Este tipo de certificado está habilitado para su uso en el sistema de información de la Cámara de Compensación de Cheques y, en particular, en el proceso de Truncamiento y Digitalización de Cheques según la normativa relacionada vigente.

Los límites de uso fijados para este tipo de certificados en el ámbito de la Cámara de Compensación de Cheques son los siguientes:

1 - Presentación de Cheques y Firma de Imágenes.
2 - Sólo para operaciones dentro del marco tecnológico del proceso de Truncamiento y Digitalización de Cheques en la Cámara de Compensación de Cheques cuyo el importe unitario representado no supere la cantidad de DOP99,999,999.

Recuperación de Datos Cifrados

A pesar de ser posible su uso 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, pudiendo ser contactado por los siguientes medios:

Correo electrónico:	info@avansi.com.do
Teléfono:	+1 809 682 3928
Dirección:	Avenida Independencia, Núm. 655 Oficina 603 - Gazcue Distrito Nacional - República Dominicana
Dirección Web:	www.avansi.com.do

2 - CLÁUSULAS GENERALES

2.1 - OBLIGACIONES

2.1.1 - Entidad de Certificación (CA)

La Entidad Certificadora AVANSI 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) Proteger los datos de creación de firma mientras estén bajo su custodia.

d) Emitir certificados conforme a esta Política y a los estándares de aplicación.

e) Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.

f) Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados cualificados.

g) Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.

h) Suspender y revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL.

i) Informar a los Firmantes/Suscriptores de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.

j) Publicar esta Política y las Prácticas correspondientes en su página web.

k) 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.

l) No almacenar ni copiar los datos de creación de firma del Firmante/Suscriptor.

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 - Unidad de Registro (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:

o) Respetar lo dispuesto en esta Política.

p) Proteger sus claves privadas.

q) Recibir las solicitudes de emisión, suspensión y revocación de certificados.

r) Verificar la exactitud y autenticidad de la información suministrada por el Firmante/Suscriptor o el solicitante.

s) Remitir las solicitudes de emisión, suspensión y revocación aprobadas a la Entidad de Certificación responsable.

t) Informar a los titulares sobre el proceso de emisión, suspensión y revocación de certificados.

u) Registrar y documentar las acciones realizadas y conservarlas.

v) Gestionar el registro de usuarios y sus solicitudes de certificación así como las respuestas a dichas solicitudes.

w) Mantener contacto directo con los usuarios y gestionar el ciclo de vida de un certificado.

x) Proteger los datos de creación de firma mientras estén bajo su custodia.

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

z) Respetar lo dispuesto en los contratos firmados con la CA y con el Firmante/Suscriptor.

aa) Informar a la CA las causas de revocación, siempre y cuando tomen conocimiento.

bb) Notificar la emisión del certificado al suscriptor titular del mismo, a quien éste señale y a terceros indicados en la presente Política de Certificación,

cc) Notificar a los suscriptores de certificados digitales emitidos por la entidad de certificación, cuando la misma decidiera cesar en el ejercicio de sus actividades.

2.1.3 - Solicitante

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

a) Brindar a la RA datos válidos, susceptibles de verificación.

b) Demostrar ser el poseedor de poderes notariales de representación de la entidad.

c) Garantizar la exactitud y veracidad de la información suministrada.

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

e) Custodiar y garantizar la protección de sus claves privadas, sus claves de activación y sus dispositivos criptográficos.

f) Solicitar la revocación o la suspensión del Certificado.

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) Utilizar sus claves y sus certificados de una manera apropiada, de acuerdo a lo establecido en la presente Política de Certificación.

b) Respetar lo dispuesto en contrato firmado con la Entidad de Certificación.

c) Informar a la Entidad de Certificación ante cualquier sospecha de vulnerabilidad o mal uso de su clave privada y solicitar la revocación de su certificado.

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.

f) No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por la CA o la RA de la suspensión o revocación del mismo, o una vez expirado el plazo de validez del certificado.

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.

c) No aceptar certificados digitales para fines no contemplados en la Política de Certificación correspondiente.

2.1.6 - 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 Firmante/Subscriptor y el solicitante.

j) Negligencia del Firmante/Subscriptor en la conservación de los datos de creación de firma, en el aseguramiento de la confidencialidad y en la protección de todo acceso o revelación del Firmante/Subscriptor.

k) Negligencia del Firmante/Subscriptor en la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.

l) Negligencia del tercero que confía en la verificación de los datos presentados en el certificado. Cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado digital publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma digital.

m) Uso de los datos de creación de firma cuando haya expirado el período de validez del certificado digital o el prestador de servicios de certificación le notifique la extinción o suspensión de su vigencia.

La CA no se responsabiliza del contenido ni el alcance de los poderes notariales del responsable de la entidad, custodio del certificado.

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 0.00 pesos dominicanos. Es decir, no se aplica ninguna

garantía de cantidad en las transacciones realizadas. Podrán 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 y renovación de certificados

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 www.avansi.com.do y/o en la de cada RA concreta.

2.5.2 - Tarifas de suspensión y revocación de certificados.

Los servicios de suspensión y revocación de certificados se ofrecerán de manera gratuita.

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 en formato digital en la página http://cps.avansi.com.do .

2.5.5 - Política de reembolso

La CA dispondrá de una política de reembolso presentada en el Contrato de Prestación de Servicio y en los Términos y Condiciones de Uso de los diversos servicios. Dichos Términos y Condiciones de Uso se pondrá a disposición del público en general en la dirección de Internet http://www.avansi.com.do y/o en la de cada RA concreta.

2.5.6 - Tarifa de legalización de documentos

La CA y sus RA's autorizadas se reservan el derecho a la aplicación de una tasa por la emisión de la documentación legalizada distinta a la ya disponible de manera pública y relativa a los aspectos de contratación de nuestros servicios.

Al mismo tiempo, se prevé la firma de documentos de carácter legal por parte de la CA o alguna de sus RA's autorizadas mediante Firma Digital en los términos recogidos en la Ley 126-02 de Comercio Electrónico, Documentos y Firma Digital, dotando a éstos de plena validez legal.

Todo ello sin perjucio de otras responsabilidades recogidas en la Ley No. 479-08 sobre Sociedades Comerciales y Ley 3-02 sobre Registro Mercantil.

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://cps.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 códigos PIN o contraseñas 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 www.avansi.com.do.

b) El listado de certificados revocados (CRL) de la CA es público, salvo lo establecido en el apartado 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 actualizará y publicará la CRL dentro de las 4 horas siguientes a la recepción de una solicitud de suspensión que haya sido previamente validada y existan indicios de su necesidad. La CRL que contiene la lista de los certificados revocados se publicará con una frecuencia mínima semanal si no se han producido cambios.

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 Instituto Dominicano de las Telecomunicaciones (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. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

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. La CA dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo que deberán firmar todas las personas que tengan acceso a información confidencial.

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

La CA no tiene responsabilidad en el caso de resolución de disputas de nombres. La asignación de nombres se realizará basándose en su orden de entrada. La CA no arbitrará este tipo de disputas que deberán ser resueltas directamente por las partes. La CA en todo caso se atiene 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 del Contribuyente (RNC).

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 la institución

La CA por si misma o a través de la RA comprobará los datos relativos a la constitución y personalidad jurídica de la entidad.

3.1.8.1 - Entidades de Intermediación Financieras (EIF)

La CA por si misma o a través de la RA comprobará los datos relativos a la constitución y personalidad jurídica de la entidad. Esta comprobación se realizará a través de las fuentes facilitadas por los órganos reguladores, Banco Central de la República y/o Superintendencia de Bancos, bien de manera online por cualquiera de los mecanismos ofrecidos por éstos en sus respectivos sitios web, o bien a partir de información remitida previamente para consulta de nuestra CA o cualquiera de las RA´s autorizadas.

La anterior comprobación podrá ser sustituida, en caso de falla en el servicio on-line, por la presentación de una copia de certificado vigente de cualquiera de las fuentes mencionadas anteriormente.

3.1.9 - Modelo Orientativo de Poder

A efectos de la emisión de este tipo de certificados se darán por válidos las autorizaciones que contengan un párrafo del siguiente tenor: “Solicitar certificados digitales de persona jurídica en representación de la entidad para la realización de firma digital y la ejecución de transacciones electrónicas, contrataciones y cualquier otra actividad que requiera del uso de la firma digital o del certificado”.

Sin embargo, la entidad certificadora se reservará el derecho de solicitar o utilizar otro tipo de documentos como sustituto del modelo descrito.

3.1.10 - Autenticación de la identidad de un individuo

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

Para acreditar la posición y poder legal del custodio sobre la institución se seguirán los siguientes parámetros:

a) Si el solicitante es un administrador o representante legal de la entidad, se exigirá la presencia física del solicitante y además la presentación del documento público donde conste el nombramiento del solicitante y su condición de administrador o representante legal.

b) Si el solicitante es un representante voluntario de la entidad con poder bastante, se exigirá la presencia física del solicitante y además la presentación del documento que acredite la autorización por parte de la entidad tal y como se describe en el apartado 3.1.9 - .

En todos los casos, para la verificación de la entidad del individuo se exigirá la presentación del documento de identidad, en original y copia, pudiendo ser aceptados la Cédula de Identidad, Cédula de Identidad y Electoral o Pasaporte.

3.1.11 - 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 dentro de un periodo de siete días naturales luego de la entrega del certificado.

Este procedimiento se aplicará en caso de que existiera alguna diferencia entre los datos suministrados a la CA y el contenido del Certificado. El Firmante/Suscriptor o su representante 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.

Las tarifas para las modificaciones realizadas en un certificado ya emitido y que aún esté vigente serán publicadas en la página web de la CA, tal y como se describe en el punto 2.5 - .

3.1.12 - 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

Las renovaciones del certificado se podrán realizar mediante correo electrónico o el acceso a la página Web de AVANSI http://www.avansi.com.do. Para ello podrá utilizarse el certificado activo.

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 o representante 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 2 años desde la última verificación de la identidad realizada mediante la personación física del representante del Firmante/Suscriptor.

3.3 - REEMISIÓN DESPUÉS DE UNA REVOCACIÓN

La CA no realizará reemisiones.

3.4 - SOLICITUD DE REVOCACIÓN

Todas las solicitudes de revocación serán autenticadas.

3.5 - PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Bajo la presente política los certificados tendrán una validez de dos (2) años.

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 presencia física del mismo o una base de datos institucional. En todos los casos se exigirá la presentación del documento de identidad, en original y copia, pudiendo ser aceptados la Cédula de Identidad, Cédula de Identidad y Electoral o Pasaporte.

d) Se registrará en todo caso:

   1. Nombre completo del Representante de la Institución, tal y como aparece en el documento de identificación presentado.

   2. Número del documento de identidad que lo acreditó.

   3. Nombre completo y forma jurídica del Firmante/Suscriptor.

   4. Evidencia de la existencia de la institución.

   5. Evidencia de los poderes notariales del representante.

e) El Solicitante o Representante facilitará 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 Solicitante o Representarte, ya sea en formato físico o digital, el cual incluirá:

   1. Solicitud del certificado digital.

   2. Copia del documento de identidad del Solicitante o Representante de acuerdo al apartado 3.1.10 - .

   3. Poderes de Representación del Solicitante o Representante.

4. Autorización de emisión del certificado de acuerdo al apartado 3.1.9 - (si procede).

5. Evidencia de existencia de la institución.

6. Texto firmado del contrato de Prestación de Servicios y anexo.

7. 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.

8. Si y bajo que condiciones el Firmante/Suscriptor consiente la publicación de su certificado.

9. 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 Firmante/Subscriptor 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 Firmante/Subscriptor 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 del mismo en función de alguna circunstancia distinta a la caducidad. 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 - Persona o institución autorizada a solicitar la suspensión o revocación

La revocación de un certificado podrá solicitarse únicamente por el representante del Firmante/Suscriptor, el solicitante del Certificado, o por la propia CA.

Todas las solicitudes serán en todo caso autenticadas.

4.4.3 - Suspensión

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

4.4.3.1 - Causas de suspensión

a) Solicitud voluntaria del Firmante/Suscriptor.

b) Iniciación del trámite de ausencia con presunción de fallecimiento del suscriptor del certificado.

c) Decisión de la Entidad de Certificación en virtud de razones técnicas. Circunstancia que será comunicada en forma inmediata en un plazo máximo de veinticuatro (24) horas al suscriptor del certificado y al INDOTEL.

d) Por cualquier duda 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.

e) Por resolución judicial o administrativa que lo ordene.

f) 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.

4.4.3.2 - Procedimiento para la solicitud de suspensión

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

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 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 correo electrónico firmado, teléfono, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

El servicio de gestión de las suspensiones 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 suspensión 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.

4.4.3.3 - 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.

4.4.3.4 - Terminación de la suspensión de un certificado

La suspensión del certificado podrá terminar en la revocación o reinserción del mismo bajo alguno de los siguientes factores:

a) Por decisión de la Entidad de Certificación de revocar el certificado, en los casos previstos en la normativa vigente.

b) Por decisión de la Entidad de Certificación de levantar la suspensión del certificado, una vez que cesen las causas que la originaron.

c) Por la decisión del suscriptor del certificado, cuando la suspensión haya sido solicitada por éste, y este hecho sea comunicado a la Entidad de Certificación.

d) Por resolución judicial o administrativa que lo ordene.

4.4.4 - Revocación

La revocación es la pérdida de validez definitiva de un certificado en función de alguna circunstancia distinta a la caducidad del mismo.

4.4.4.1 - Causas de revocación

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

a) Solicitud voluntaria del Firmante/Suscriptor a través de su representante.

a) Solicitud voluntaria del solicitante.

b) Pérdida o inutilización por daños del soporte del certificado.

c) Por la extinción de la institución.

d) Por solicitud de la Entidad de Certificación, la Unidad de Registro

e) Fallecimiento del Firmante/Suscriptor o incapacidad sobrevenida, total o parcial.

f) Terminación de la vinculación del representante con la institución o pérdida de los poderes de representación correspondientes.

g) Cese en la actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.

h) 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.

i) 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.

j) Por incumplimiento por parte de la RA, CA o el Firmante/Suscriptor de las obligaciones establecidas en esta política.

k) Por la resolución del contrato con el Firmante/Suscriptor.

l) Por resolución judicial o administrativa que lo ordene.

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

n) 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.

4.4.4.2 - 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 laborables.

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 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 una visita personalmente o mediante comunicación por correo electrónico firmado, teléfono, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

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

Cuando se usen listas de certificados revocados (CRLs) que incluyan algunas variantes, 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.

4.4.4.3 - Límite del periodo de revocación

La decisión de revocar o no un certificado no podrá retrasarse por un periodo máximo de cinco (5) días laborables.

4.4.5 - Frecuencia de emisión de CRL's

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

La CA actualizará y publicará la CRL dentro de las 4 horas siguientes a la recepción de una solicitud de suspensión o revocación que haya sido previamente validada, y al menos con una frecuencia diaria si no se han producido cambios en la CRL.

4.4.6 - Requisitos de comprobación de CRL's

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

La verificación de los validez de los certificado es responsabilidad del tercero.

4.4.7 - Disponibilidad de comprobación on-line de la revocación

CA proporciona un servicio on-line de comprobación de revocaciones a través de la emisión de CRL. Estos servicios estarán disponibles las 24 horas del día los 7 días de la semana en la siguiente dirección: http://services.avansi.com.do/ocsp

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.

4.4.8 - Requisitos de la comprobación de la revocación

El tercero que confía que desee comprobar la suspensión o revocación de un certificado, podrá hacerlo consultando las CRLs a través de la página web de la CA www.avansi.com.do o mediante el servicio online descrito en el punto anterior de forma gratuita. No obstante lo anterior, el acceso a este sistema de consulta de certificados podrá restringirse según lo establecido en el apartado 2.5.3 - .

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. Copia del documento de identidad del Solicitante o Representante de acuerdo al apartado 3.1.10 - .

   3. Contrato de Prestación de Servicios y anexo.

   4. Algunas cláusulas específicas contenidas en el contrato.

   5. Método empleado para comprobar la validez del documento de identidad, 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 y a su Representante.

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 4.5 - 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 - 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) Documentación requerida por los auditores.

g) Historial de claves generadas.

h) 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 4.5.1 - en sus incisos 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 10 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

La CA dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido sólo al personal autorizado.

4.6.5 - 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 restablecer 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 restablecimiento.

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 CA's 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. Éstas 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 aún no ha expirado.

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

Todos los controles técnicos y de seguridad aplicables a la presente Política están extendidos de las CPS (Certification Practice Statement) que regulan el funcionamiento operacional de la CA.

Las CPS están disponibles en http://cps.avansi.com.do

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 mediante un sistema confiable. 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.

El Firmante/Subscriptor entiende que no debe revelar su clave privada a terceros bajo ninguna circunstancia y debe almacenarla en un medio que garantice su confidencialidad.

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 o bien en un medio software.

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, 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.

c) El proveedor de la clave pública es el legítimo Firmante/Suscriptor 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 - Disponibilidad de la Clave Pública de la Entidad de Certificación

La clave pública de la CA (certificado raíz) y su fingerprint (huella digital) estará a disposición del público en general en la página de Internet de la CA www.avansi.com.do y del órgano regulador de la CA, INDOTEL.

6.1.7 - 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 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.

b) El periodo máximo de validez de los certificados de los Firmantes/Suscriptores firmados con esa clave.

6.1.8 - Tamaño y periodo de validez de las claves del Firmante/Suscriptor

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

El periodo de uso de la clave pública y privada del Firmante/Suscriptor es de dos (2) años pudiendo ser renovada por no más de tres períodos. El mismo no excederá del periodo durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

6.1.9 - Requisitos para la generación de las 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 hardware criptográfico.

6.1.10 - Fines del uso de las claves

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 y para los usos descritos en el apartado 1.4.7 - .

6.2 - PROTECCIÓN DE LA CLAVE PRIVADA

6.2.1 - De la CA y las RA

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. Esto es asimismo aplicable a las RA's en relación con las claves privadas que emplean en sus procedimientos de aprobación.

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.

6.2.2 - 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:

a) El Firmante/Suscriptor pueda mantener la clave privada bajo su exclusivo control.

b) Su secreto está razonablemente asegurado.

c) La clave privada puede ser efectivamente protegida por el Firmante/Suscriptor contra un uso ajeno.

d) No podría ejecutarse una recuperación (“escrow”) de claves privadas, es decir, que no se permite que terceros puedan legalmente obtener la clave privada sin el consentimiento del suscriptor del certificado correspondiente.

Todo Firmante/Suscriptor podrá, a su criterio, mantener una copia de resguardo o back-up de su propia clave privada. Sin embargo, bajo ninguna circunstancia, la Entidad de Certificación mantendrá una copia de la clave privada del Firmante/Suscriptor de un certificado emitido bajo esta Política.

6.3 - ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Todos los estándares técnicos y de seguridad aplicables a la presente Política están extendidos de las CPS (Certification Practice Statement) que regulan el funcionamiento operacional de la CA.

Las CPS están disponibles en http://cps.avansi.com.do

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 luego de su expiración o revocación por el plazo mínimo establecido en la legislación vigente, a fin de posibilitar la verificación de firmas digitales generadas durante su plazo de vigencia.

6.4.2 - Periodo de uso para las claves públicas y privadas

Descrito en los apartados 6.1.7 - y 6.1.8 - .

6.4.3 - Reemplazo de claves

El par de claves de la Entidad de Certificación serán reemplazadas cuando las mismas hayan sido vulneradas o exista presunción en tal sentido, siguiendo el apartado 4.8.1 - .

6.4.4 - Restricciones al uso de claves privadas

Descrito en el apartado 6.1.10 - .

6.5 - Datos de Activación

Los datos de activación son aquellos valores distintos a las claves criptográficas, que se requieren para operar módulos criptográficos, y que deben ser protegidos de accesos no autorizados. Los datos de activación deben ser únicos y aleatorios.

6.6 - CICLO DE VIDA DEL DISPOSITIVO SEGURO DE ALMACENAMIENTO DE LOS DATOS DE CREACIÓN DE FIRMA (DSADCF) Y DEL DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA (DSCF)

La 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.

6.7 - 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

6.7.1 - 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.

6.8 - CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.8.1 - Controles de desarrollo del sistema

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

6.8.2 - Controles de gestión de la seguridad

6.8.2.1 - 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 concientización 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.

6.8.2.2 - 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.

6.8.2.3 - 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.

Planificación 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) La CA define actividades, asignadas a personas con un rol de confianza, distintas a las personas encargadas de realizar las operaciones cotidianas que

no tienen carácter de confidencialidad. Las operaciones de seguridad de la CA serán separadas de las operaciones normales.

6.9 - CONTROLES DE SEGURIDAD DE LA RED

6.9.1 - 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 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.

6.9.2 - Gestión de la revocación

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.

6.9.3 - 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.
e) La clave privada de firma de la CA almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

6.10 - CONTROLES DE SEGURIDAD DE LA RED

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

La información confidencial que se transfiere por redes no seguras se realiza de forma encriptada.

6.11 - CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

Todas las operaciones criptográficas de la CA son realizadas en un módulo validado por FIPS 140-1 nivel 2 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

AVANSI emite certificados X.509 versión 3. Lo cual se indicará en el campo versión.

7.1.2 - Extensiones del certificado CEIF-PJ (Certificado de Entidad de Intermediación Financiera – Persona Jurídica)

EXTENSIÓN		VALOR
Versión		V3
Número de serie		<núm. serie>
Algoritmo de firma		sha1RSA
Emisor	C	DO
	L	DISTRITO NACIONAL REPUBLICA DOMINICANA
	O	AVANSI S.R.L - 130222509
	CN	AVANSI CERTIFICADOS DIGITALES
Válido desde		<fecha inicio validez>
Válido hasta		<fecha fin validez>
Asunto	1.3.6.1.4.1.27395.8.3	<email del representante>
	1.3.6.1.4.1.27395.8.2	<id del representante: cédula>
	1.3.6.1.4.1.27395.8.1	ENTIDAD INTERMEDIACION FINANCIERA – PERSONA JURIDICA
	C	Country <DO>
	L	Location <ciudad de la EIF>
Asunto	O	Organization <razón social de la EIF>
	T	Title <cargo del representante>
	SN	Serial Number <RNC de la EIF>
	GN	Given Name <nombre del representante>
	SurName	<apellido del representante>
	CN	Common Name <nombre de la EIF o departamento>
	UID	Userid <código BIC / SWIFT de la EIF>
	Initials	<tipo de EIF: lista de valores: Asociación de Ahorro y Préstamos, Bancos de Ahorro y Crédito, Bancos Múltiples>
Clave Pública		RSA (2048 Bits)
Uso mejorado de claves		Autenticación del cliente (1.3.6.1.5.5.7.3.2) Firma de código (1.3.6.1.5.5.7.3.3) Correo seguro (1.3.6.1.5.5.7.3.4)

EXTENSIÓN	VALOR
Certificate Subject Key ID	08 5f 8a 6f 1b 74 11 e7 5a 92 ef 61 6e 9b e2 61 cb a3 f1 19
Certificate Subject Key ID	Id. de clave=5c ab c7 97 fd 42 2e 3d d3 89 e3 a5 cb 6d 2f 7e 05 a2 e5 cc
Nombre alternativo del sujeto	Nombre RFC822: <email de la EIF>
	1.3.6.1.4.1.27395.8.4: altName1: <Operaciones Permitidas>
	1.3.6.1.4.1.27395.8.5: altName2: Límites de uso>
Bases del certificado	[1] Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.27395.6.2.5 [1,1]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Este es un certificado para Entidad de Intermediación Financiera (EIF). El tipo de EIF y el Código BIC están informados en los campos INITIALS y UID respectivamente. El alcance está recogido en los atributos AltName1 y AltName2. [1,2]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://cps.avansi.com.do
Puntos de distribución CRL	[1] Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección: *URL*=http://crl.avansi.com.do/avansidigitalcertificate.crl [2] Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección: *URL*=http://crl2.avansi.com.do/avansidigitalcertificate.crl

EXTENSIÓN	VALOR
Acceso a la información de entidad emisora	[1] Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección: *URL*=http://services.avansi.com.do/ocsp

7.1.3 - Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma será el SHA-1 with RSA Encryption 1.2.840.113549.1.1.5.

El identificador de objeto del algoritmo de la clave pública será RSA Encryption 1.2.840.113549.1.1.1

7.2 - PERFIL DE CRL

VERSIÓN		V2
Emisor	C	DO
	L	DISTRITO NACIONAL REPUBLICA DOMINICANA
	O	AVANSI S.R.L - RNC 130222509
	CN	AVANSI CERTIFICADOS DIGITALES
Periodo máximo de validez		1 día
Algoritmo de firma		sha1RSA
Identificador de clave de autoridad		Id. de clave= 5c ab c7 97 fd 42 2e 3d d3 89 e3 a5 cb 6d 2f 7e 05 a2 e5 cc
URL de distribución		http://crl.avansi.com.do/avansidigitalcertificate.crl http://crl2.avansi.com.do/avansidigitalcertificate.crl

7.2.1 - Número de versión

Las CRL emitidas por AVANSI son de la versión 2. Lo cual se indicará en el campo versión.

8 - ESPECIFICACIÓN DE LA ADMINISTRACIÓN

8.1 - AUTORIDAD DE LAS POLÍTICAS

La Gerencia de AVANSI 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.

En la web de AVANSI 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://cps.avansi.com.do

8.4 - PROCEDIMIENTOS DE APROBACIÓN DE LA POLÍTICAS

Para la aprobación y autorización de las Políticas se respetarán los procedimientos especificados por la PA. La publicación de las revisiones de esta Política deberá estar aprobada por la PA.