Prácticas de Certificación

CPS - Avansi

v2.3

ÍNDICE

CONTROL DE DOCUMENTO

Título:	Prácticas de Certificación		
Asunto:	CPS - Avansi		
Autor:	Avansi, Entidad de Certificación		
Versión:	v2.3	**Fecha:**	15-03-2013
Código:	AVS-CPS	**Última revisión:**	21-09-2009
Idioma:	Español	**Núm. Páginas:**	69

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	**Versión**	**Motivo del Cambio**
20-08-09	2.1	• Adición del inciso d (capítulo 2.1.3) • Adición de los incisos a, b, c, e y g (capítulo 2.1.4) • Adición del inciso c (capítulo 2.1.5) • Adición del inciso f (capítulo 2.2) • Adición de los incisos j, k, l, y m (capítulo 2.2.1) • Adición del capítulo 2.5.2 • Redefinición de la política de reembolso (capítulo 2.5.5) • Redefinición de difusión de los certificados (capítulo 2.6.1.3) • Actualización de los tipos de nombres admitidos (capítulo 3.1.1) • Incremento de los métodos utilizados para solicitar (capítulo 4.1) • Adición del capítulo 4.1.1 • Descripción exhaustiva del proceso de emisión (capítulo 4.2) • Incremento de los métodos utilizados para solicitar (capítulo 4.4.3) • Adición del capítulo 4.4.4 • Estandarización del tiempo de actualización de la CRL (capítulo 4.4.6) • Reducción del período de almacenamiento (capítulo 4.6.2) • Cambio en el período de uso de una clave privada de la CA (capítulo 6.1.5). • Definición del tiempo de retención de archivos (capítulo 6.4.1) • Adición del capítulo 6.4.3
21-09-09	2.2	Actualización de datos de contacto (capítulo 1.5)
18-06-13	2.3	Punto 1.2.1: actualización profiles. Punto 1.5: actualización datos de contacto. Punto 2.1.7: actualización CRLs y OCSP. Punto 2.6.2: actualización frecuencia de publicación CRLs. Punto 3.1.1: tipos de nombres; se referencia a las CPs. Punto 3.1.7: actualización procedimiento creación de claves. Punto 4.4.6: actualización frecuencia de publicación CRLs. Punto 4.4.8: actualización datos OCSP. Punto 5: actualización generalidades del CPD. Punto 6.1.1: actualización prestaciones HSM. Punto 6.1.7: actualización prestaciones HSM. Punto 6.2.1: actualización prestaciones HSM. Punto 6.2.2: actualización URL para FAQs de la web de avansi. Punto 6.5.1: Revisión dispositivos hardware. Punto 6.10: actualización prestaciones HSM.

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 Declaración de Prácticas de Certificación de CA AVANSI para la emisión de certificados, y está basada en la especificación del estándar RCF 2527 – Internet X. 509 Public Key Infrastructure Certificate Policy, de IETF, RFC 3039 del IETF y ETSI TS 101 456 V1.2.1. y en las propias políticas de certificación, siguiendo su misma estructura.

Esta CPS se encuentra en conformidad con las Políticas de Certificación de los diferentes certificados emitidos por CA AVANSI CERTIFICACIÓN. En caso de contradicción entre los dos documentos prevalecerá lo dispuesto en las Políticas de Certificación concretas.

La utilización de jerarquías permite reducir los riesgos asociados a la emisión de certificados y distribuir comunidades y usos de certificados en diferentes CA's. AVANSI emite certificados de usuario final desde la CA AVANSI Certificados Digitales.

1.2.1. Jerarquía AVANSI CERTIFICACIÓN

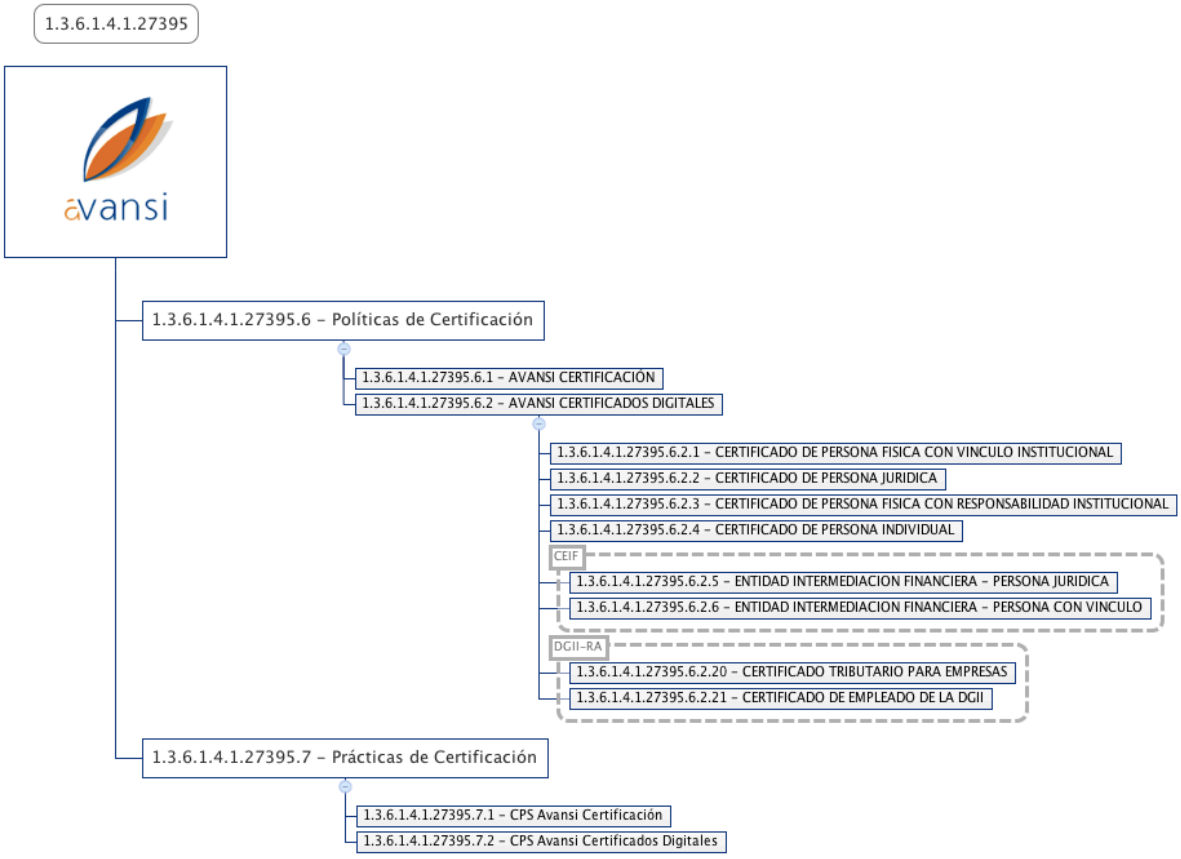
Esta Jerarquía esta diseñada para construir una red de confianza donde las Autoridades de Registro son gestionadas por AVANSI o entidades que hayan firmado un convenio de representación con AVANSI, teniendo como objetivo fundamental la emisión de certificados digitales de usuario basados en las políticas correspondientes a cada uno.

De la Entidad Raíz de esta Jerarquía, AVANSI Certificación, cuelga una CA intermedia que pertenece a la CA AVANSI Certificación y que emite certificados digitales en el ámbito de la República Dominicana es una Entidad de Certificación multipolítica, AVANSI Certificados Digitales, emitiendo distintos profiles de certificados de usuario, tal y como se describe en sus respectivas CP (Certificate Policies).

La actividad de la Entidad de Certificación podrá ser sometida a la inspección de la Autoridad de Políticas (PA) o por personal delegado por la misma sin perjuicio de someterse a todas las auditorías externas que sean aplicables conforme lo dicta la norma complementaría sobre auditoría aprobada por la autoridad reguladora Instituto Dominicano de Telecomunicaciones (INDOTEL).

La gerencia de AVANSI constituye la Autoridad de Políticas (PA) de la Jerarquía y de las Entidades de Certificación descritas anteriormente siendo responsable de la administración de la CPS. Puede contactar con la Autoridad de Políticas (PA) en el correo electrónico: info@avansi.com.do

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


1.3.6.1.4.1.27395
avansi
1.3.6.1.4.1.27395.6 – Políticas de Certificación
1.3.6.1.4.1.27395.6.1 – AVANSI CERTIFICACIÓN
1.3.6.1.4.1.27395.6.2 – AVANSI CERTIFICADOS DIGITALES
1.3.6.1.4.1.27395.6.2.1 – CERTIFICADO DE PERSONA FISICA CON VINCULO INSTITUCIONAL
1.3.6.1.4.1.27395.6.2.2 – CERTIFICADO DE PERSONA JURIDICA
1.3.6.1.4.1.27395.6.2.3 – CERTIFICADO DE PERSONA FISICA CON RESPONSABILIDAD INSTITUCIONAL
1.3.6.1.4.1.27395.6.2.4 – CERTIFICADO DE PERSONA INDIVIDUAL
CEIF
1.3.6.1.4.1.27395.6.2.5 – ENTIDAD INTERMEDIACION FINANCIERA – PERSONA JURIDICA
1.3.6.1.4.1.27395.6.2.6 – ENTIDAD INTERMEDIACION FINANCIERA – PERSONA CON VINCULO
DGII-RA
1.3.6.1.4.1.27395.6.2.20 – CERTIFICADO TRIBUTARIO PARA EMPRESAS
1.3.6.1.4.1.27395.6.2.21 – CERTIFICADO DE EMPLEADO DE LA DGII
1.3.6.1.4.1.27395.7 – Prácticas de Certificación
1.3.6.1.4.1.27395.7.1 – CPS Avansi Certificación
1.3.6.1.4.1.27395.7.2 – CPS Avansi Certificados Digitales

1.3. Identificación

La presente Declaración de Practicas de Certificación está identificada con el OID:

1.3.6.1.4.1.27395.7.1

ISO (1)
ORG (3)
DOD (6)
Internet (1)
Private (4)
Enterprise (1)
AVANSI (27395)
Prácticas de Certificación (7)
CA AVANSI Certificación (1)

1.4. Comunidad y Ámbito de Aplicación

1.4.1. Entidad de Certificación (CA)

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

La información relativa a la CA puede encontrarse en la dirección Web www.avansi.com.do.

1.4.2. Prestador de Servicios de Certificación

Entendemos bajo la presente CPS a un PSC como aquella entidad que presta los servicios concretos relativos al ciclo de vida de los certificados. Las funciones de PSC pueden ser desempeñadas directamente por la CA o por una entidad delegada. A los efectos de la presente CPS la propia AVANSI será el PSC.

1.4.3. Autoridad de Registro (RA)

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

A los efectos de la presente CPS podrán actuar como RA's las oficinas de AVANSI y aquellas entidades que hayan suscrito acuerdos al respecto con la CA y superado los cursos y auditorías exigidas en las Políticas de Certificación.

1.4.4. Firmante o Suscriptor

Entendemos por Firmante/Suscriptor al titular del certificado. De acuerdo a la presente CPS podrán emitirse certificados digitales de AVANSI:

a) Direcciones Internet para el establecimiento de canales seguros SSL.

b) Una persona física con una vinculación contractual con una institución con personalidad jurídica.

c) Una persona física con una vinculación contractual con una institución con personalidad jurídica que le atribuye ciertos poderes legales.

d) Una persona jurídica.

1.4.5. Tercero que Confía

En esta CPS se entiende por Tercero que confía, la persona que voluntariamente confía en el Certificado de AVANSI, en virtud de la confianza depositada en la CA.

1.4.6. Solicitante

Se entenderá por Solicitante la persona física que solicita el Certificado y que:

a) En el caso del certificado del servidor, es el responsable administrativo o técnico que figura en las bases de datos de los dominios.

b) En los casos de certificados de personas físicas, es la persona física o institución que solicita el certificado, y que en el contexto sus Política, puede coincidir con la figura del Firmante/Suscriptor.

c) En el caso de certificados de personas jurídicas, es la persona física que solicita el Certificado, responsable de la custodia del mismo. El solicitante de un certificado de persona jurídica podrá los administradores y representantes legales de la institución.

1.4.7. Institución

Se entenderá por Institución a la persona jurídica:

a) En el caso del certificado del servidor,

b) En los casos de certificados de personas físicas, es aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el Firmante/Suscriptor.

c) En el caso de certificados de personas jurídicas, es la entidad que solicita el certificado, y que en el contexto sus Política, puede coincidir con la figura del Firmante/Suscriptor.

1.4.8. Ámbito de Aplicación y Usos

Esta CPS da respuesta a las Políticas de Certificación descritas en el apartado **¡Error! No se encuentra el origen de la referencia.** de la presente CPS. Los certificados de la CA AVANSI podrán usarse en los términos establecidos por las Políticas de Certificación correspondientes.

1.4.8.1. Usos Prohíbidos 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 de la CA

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

Razón Social:	Avansi, S.R.L. RNC 130 222 509
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 CPS y en las Políticas de Certificación.

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 CPS, a las Políticas de Certificación 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 CPS 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 CPS y las Políticas correspondientes en su página web.

k) Informar sobre las modificaciones de esta CPS y a las Política 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:

a) Respetar lo dispuesto en esta CPS y en las Políticas de Certificación.

b) Proteger sus claves privadas.

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

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

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

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

f) Registrar y documentar las acciones realizadas y conservarlas.

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

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

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

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

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

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

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

n) 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) Suministrar a la RA la información necesaria para realizar una correcta identificación.

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

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

d) Demostrar ser el poseedor de poderes notariales de representación de la entidad (si procede).

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

f) Solicitar la revocación o la suspensión del Certificado (si procede).

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

b) Custodiar y garantizar la protección de sus claves privadas, sus claves de activación y sus dispositivos criptográficos, si los tuviera.

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

d) Respetar lo dispuesto en contrato firmado con la CA y la RA.

e) 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.

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

g) 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. Institución

En el caso de los certificados de persona física, será obligación de la Institución solicitar a la RA la suspensión/revocación del certificado cuando cese la relación del Firmante/Suscriptor con la organización.

2.1.7. Repositorio

La información relativa a la revocación / suspensión de los certificados se mantendrá accesible al público en los términos establecidos en la normativa vigente. La CA AVANSI ofrece dos mecanismos de consulta de certificados revocados:

Mediante la consulta de CRLs:

- http://crl.avansi.com.do/avansisub.crl
- http://crl2.avansi.com.do/avansisub.crl

y mediante la consulta online, basado en el protocolo OCSP (RFC6960), que ofrece el estado en tiempo real.

- http://ocsp.avansi.com.do

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. Esta información es custodiada con medidas de integridad y acceso que garantizan su integridad de acuerdo con las exigencias de las Políticas de Certificación.

2.2. Responsabilidad

La CA será responsable de los daños y perjuicios ocasionados a los usuarios de sus servicios, ya sea el Firmante/Suscriptor o el Tercero que confía en los términos establecidos en la legislación vigente y en las Políticas de Certificación.

En cumplimiento de la legislación vigente AVANSI dispone de un seguro de responsabilidad civil con una cobertura de ochenta mil dólares de los Estados Unidos de América (US$ 80,000.00), o su equivalente en moneda de la República Dominicana.

La CA también será responsable 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.

f) Por la inexactitud de los datos que consten en el certificado digital, si éstos le han sido acreditados mediante documento público.

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.

2.2.2. Límite de responsabilidad en caso de pérdidas por transacciones

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

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

2.3. Responsabilidad Financiera

AVANSI en su actividad como PSC, dispone de un seguro de responsabilidad civil que contempla sus responsabilidades, para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios: el Firmante/Suscriptor y el Tercero que confía por un importe conjunto máximo de ochenta mil dólares de los Estados Unidos de América (US$ 80,000.00), o su equivalente en moneda de la República Dominicana.

2.4. Interpretación y Ejecución

2.4.1. Legislación

La ejecución, interpretación, modificación o validez de las presentes CPS 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 a la CPS 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 de Servicios

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://politicas.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.

2.6. Publicación y Repositorio

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 CPS es pública y se encuentra disponible en el sitio de Internet http://politicas.avansi.com.do

2.6.1.2. Términos y Condiciones

La CA o la RA pondrán a disposición de los Firmantes/Suscriptores y Terceros que confían los términos y condiciones del servicio antes de proceder a la emisión del certificado o de entregar los 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 epígrafe 2.5.3.

c) La CA pondrá a disposición de los Terceros que confían los Términos y Condiciones referentes al uso de los certificados.

La información a la que se refieren los 2 primeros puntos estará disponible 24 horas al día, 7 días por semana. En caso de fallo del sistema u otros factores que no se encuentran bajo el control de la CA, la CA hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

2.6.2. Frecuencia de Publicación

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

La CA publicará las CRLs con una frecuencia de 24 horas, pudiéndose publicar de manera extraordinaria en cualquier momento en caso de ser aprobado por la Autoridad de Políticas ante cualquier eventualidad que así lo recomiende.

Al mismo tiempo, la CA ofrece el servicio de validación online, basado en el protocolo OCSP (RFC6960), que ofrece el estado en tiempo real.

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 emplea su página Web para la solicitud de certificados y distribución de las CRL's. Se empleará por lo tanto un protocolo HTTP para acceder a la lista de revocación.

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. Auditorías

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 CPS y en las Política 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 estas CPS siempre que no contravengan ni la normativa vigente ni lo dispuesto en las 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. Envio de información a la Autoridad de 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 de las presentes CPS y del sistema de certificación que regulan las Política de Certificación generadas por esta.

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.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Registro Inicial

3.1.1. Tipos de nombres

El Firmantes/Suscriptor se describe en los certificados mediante un nombre distintivo (DN o distinguished name) conforme al estándar X.500.

El formato DN del Firmante/Suscriptor del certificado se explica y describe en las CP de cada profIle.

3.1.2. Pseudónimos

La admisión o no de pseudónimos es tratada en cada una de las Políticas de Certificación.

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 (cédula de identidad, cédula de identidad y electoral, pasaporte o RNC) 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 **¡Error! No se encuentra el origen de la referencia.** 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). La CA no asume compromisos en la emisión de certificados respecto al uso de una marca comercial.

La CA no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del Firmante/Suscriptor. Sin embargo, la CA no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

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

La CA emplea diferentes circuitos donde la clave privada es gestionada de diferente manera. La Jerarquía utilizada permite realizar la generación de las claves de diferentes modos:

a) **Generación de claves por parte de AVANSI.** Se entregan al suscriptor mediante ficheros protegidos utilizando el estándar PKCS#12 en mano o descargados a través de Internet. La

seguridad del proceso queda garantizada ya que la clave de acceso al fichero que permitirá la instalación de éste en las aplicaciones es creada y gestionada de forma separada por el Firmante/Suscriptor y ni AVANSI ni la RA tienen acceso a ella.

Las claves pueden ser entregadas al Firmante/Suscriptor en una tarjeta criptográfica (DSCF) por la RA. En este caso las claves son generadas por AVANSI y la custodia se realiza en un dispositivo hardware.

b) **Generación de las claves por el usuario.** En este caso el usuario dispone de un mecanismo de generación de claves ya sea software o hardware. La prueba de posesión de la clave privada en estos casos es la petición recibida del suscriptor en formato PKCS#10.

3.1.8. Autenticación de la identidad de un individuo, organización y su vinculación

Para realizar una correcta identificación de la identidad del suscriptor, la CA a través de la RA exige:

a) La personación física del Firmante/Subscriptor o su Representante en posesión de un documento de identidad válido de acuerdo a las políticas correspondiente o contra una base de datos institucional, según el tipo de certificado.

b) Identificación de la institución, para lo que la RA requerirá la documentación pertinente dependiendo del tipo de entidad y por un medio conforme a Derecho. Esta información está incluida en los Manuales operativos de la RA y en las políticas particulares de cada certificado.

c) La documentación que pruebe la vinculación del Firmante/Suscriptor respecto con la institución (si procede).

Las diversas políticas y Manuales de la RA definen con detalle la documentación requerida para la emisión de cada tipo de certificado.

Para los certificados de servidor seguro, la identidad de suscriptor se comprueba mediante el acceso a las bases de datos de dominios Internet y los certificados se entregan con la autorización de los responsables que aparecen en dichas bases de datos. En los casos de certificados de servidor seguro, AVANSI no gestiona las claves privadas sino que recibe una petición en formato PKCS#11 del Solicitante.

3.2. Renovación de la Clave y del Certificado

La CA no realiza renovaciones de certificados de servidor seguro.

Las renovaciones de certificados usuarios (personas) 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 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 un período superior al definido en las políticas correspondientes. A partir de esta fecha se realizará una verificación de la identidad realizada mediante la personación física del Firmante/Subscriptor o el Solicitante, según sea el caso.

3.3. Reemisión Después de una Revocación

La CA no realizará reemisiones.

3.4. Solicitud de Revocación

La forma de realizar las solicitudes de revocación se establecen en el apartado 4.4.5.

3.5. Período de Validez de los Certificados

El período de validez de los certificados se definen en las Políticas de Certificación correspondientes.

4. REQUERIMIENTOS OPERACIONALES

4.1. Solicitud de Certificados

Las RA's gestionan las solicitudes de certificados. Las solicitudes en todo caso se realizan mediante el acceso a los formularios de solicitud en la dirección http://www.avansi.com.do, a través de correo electrónico o personalmente.

El Solicitante completará un formulario de acuerdo al método de solicitud escogido.

Se establecen también circuitos de solicitud mediante lotes.

Esta forma de petición no excluye la personación física del Firmante/Subscriptor o su representante ante la RA para aquellos certificados que así lo requieran en sus Políticas.

En estos casos será la RA la que se trasladaría a las instalaciones físicas de la entidad.

En el caso del circuito de lotes, se enviará una solicitud especial a la institución o solicitante que se completaría con los datos de los Firmantes/Subscriptores y la RA procederá a la carga de una sola vez dichas peticiones en el sistema.

Las solicitudes también pueden realizarse en el caso de certificados de servidor seguro así como en aquellos circuitos que implique la creación de la clave por el suscriptor ya sea en software o hardware, mediante envío de peticiones estandarizadas PKCS#10.

Las solicitudes también se pueden realizar mediante un certificado digital activo. Y así, en el caso de solicitar un certificado reconocido con otro certificado reconocido, no sería requisito necesario la personación física del solicitante ante la RA siempre que se cumplan los requerimientos marcados en la legislación vigente.

4.1.1. Normas generales para las solicitudes

La CA realizará los esfuerzos que razonablemente estén a su alcance para asegurar que:

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) La información presentada en las solicitudes se recogerá con el debido consentimiento del interesado y únicamente para los fines propios del servicio solicitado.

c) La información presentada en las solicitudes sólo serán tratadas por la Unidad de Registro y Entidad de Certificación de AVANSI para el servicio correspondiente correspondiente.

d) Las notificaciones relacionadas con las solicitudes y los cambios de estatus de los certificados se comunicarán a través de un medio de comunicación perdurable, susceptible de ser transmitido electrónicamente y en un lenguaje comprensible.

e) Si la solicitud cumple con los requisitos establecidos en el Manual Operativo, las Políticas y Declaración de Prácticas de la entidad la solicitud será admitida a trámite.

f) Solo serán procesadas las solicitudes que estén correctamente completadas y hayan sido verificadas con el solicitante.

g) Si alguna solicitud no hubiera sido admitida a trámite, de igual manera el solicitante recibirá en su correo electrónico esta notificación.

h) Todas las solicitudes estarán identificadas con un número de seguimiento o cod-tracking.

i) En caso de que una solicitud tenga algún tipo de error en su contenido se procederá a contactar al solicitante o subscriptor para solicitar las correcciones necesarias. Si se pueden aportar los datos individualmente, el mismo correo del solicitante donde se aporta las correcciones servirá para completar o corregir la solicitud por parte del REGISTRADOR. Dicho correo será almacenado en el formato establecido por la CA.

4.2. Emisión de Certificados

Para la emisión de certificados digitales, la CA por sí misma o por medio de la RA realizará las siguientes actividades:

a) Comprobará la identidad y los atributos específicos del Firmante/Suscriptor basado en el proceso de acreditación[1] descrito en el Manual Operativo correspondiente. 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 el Pasaporte.

b) Registrará los datos, búsquedas y documentos correspondientes de acuerdo a las Políticas de Certificación específicas. Todas la documentación generada con fines de acreditación se almacenaran en el formato establecido por la CA.

1 La Unidad de Registro, representada por el registrador se reservará el derecho de acreditar o no la identidad del solicitante o subscriptor en función de la documentación presentada.

c) Si la acreditación es correcta, se procederá a la firma y entrega del Contrato de Prestación de Servicios y sus anexos de acuerdo a las Políticas de Certificación específicas.

d) Se generará y entregará la clave:

1. Si la clave ha sido generada por el Firmante/Suscriptor, se emite de forma automática el certificado y se proporciona un enlace para la descarga del certificado desde la ubicación elegida por el suscriptor.

2. Si la clave ha sido creada por AVANSI hará llegar al Firmante/Suscritor:

   - Un enlace a la página donde se generará el certificado en formato PKCS#12 o el certificado correspondiente.

   - Un PIN necesario para la instalación de las claves y el certificado. El Firmante/Subscriptor necesitará también para el proceso de creación de las claves y el certificado, un código que se le proporciona al momento de la solicitud.

En el caso de los certificados de servidor seguro el proceso de emisión se realiza de forma automática, de tal manera que una vez se ha producido el pago del servicio se emite el certificado y se envía a los contactos administrativo y/o técnico que aparecen en las bases de datos de los dominios.

4.3. Aceptación de Certificados

Un certificado se entenderá aceptado según lo estipulado en las Políticas de certificación correspondiente.

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.

La extinción de la vigencia de un certificado electrónico por causa de revocación o suspensión producirá efectos frente a terceros desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

4.4.2. Causas de suspensión o revocación y documentos justificativos

Los certificados deberán ser revocados o suspendidos cuando concurra alguna de las circunstancias especificadas en la Política de certificación correspondiente.

Para justificar la necesidad de revocación o suspensión que se alega se deberán presentar ante la RA los documentos correspondientes, si procede, en función de la causa que motiva la solicitud.

4.4.3. Persona o institución autorizada a solicitar la suspensión o revocación

La revocación de un certificado podrá solicitarse por el Firmante/Suscriptor, su representante o la propia CA.

Para los certificados de persona física, también podrán solicitar la revocación o suspensión la empresa solicitante del certificado, la oficina de dependencia a la que se vincula el Firmante/Subscriptor o su representante. Las solicitudes deberán realizarse:

a) Por medios digitales. Mediante el acceso a los formularios de solicitud en la dirección http://www.avansi.com.do o a través de un correo electrónico.

b) A través de la personación física del Firmante/Suscriptor o su representante en la RA en horario de atención al público mostrando el documento de identidad correspondiente.

c) Por medio de una llamada a la RA en el teléfono: +1 (809) 563 4941, únicamente es recomendable en aquellos casos en que, habiendo un compromiso grave de las claves y/o el certificado, no se pudiera usar uno de los dos métodos anteriores. En este caso el solicitante deberá responder a algunas preguntas para acreditar su identidad.

Todas las solicitudes serán en todo caso autenticadas.

4.4.4. Suspensión

El procedimiento de suspensión se realiza a partir de alguno de los medios descritos en el apartado 4.4.3.

La suspensión, a diferencia de la revocación, supone la pérdida de validez temporal de un certificado, mientras se acredita la autenticidad de la solicitud de revocación recibida y se decide acerca de la activación o revocación definitiva.

En el caso de la suspensión del certificado, se enviará un comunicado al Firmante/Suscriptor comunicando la hora de suspensión y la causa de la misma.

4.4.4.1. Límite del período de revocación

La CA supervisará mediante un sistema de alertas de la plataforma de gestión de certificados que el periodo de suspensión marcado por las Políticas correspondientes y esta CPS no se sobrepasa.

4.4.5. Procedimiento de solicitud de revocación

El procedimiento de revocación se realiza a partir de alguno de los medios descritos en el apartado 4.4.3.

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.

Al momento de solicitud de la revocación se podrá suspenderá el certificado implicado de manera inmediata. El Firmante/Suscriptor cuyo certificado haya sido suspendido o revocado será informado del cambio de estado de su certificado. Así mismo, el Firmante/Suscriptor será informado del levantamiento de la suspensión.

Todas las solicitudes serán autenticadas mediante los procesos descritos en el Manual Operativo correspondiente. La solicitud podrá realizarse bajo los siguientes escenarios:

a) **Con certificado.** No requiere proceso de acreditación. La CA autenticará la solicitud confirmando la validez de la firma y si la misma se encuentra en poder del Firmante/Subscriptor o su representante.

b) **Sin certificado.** Requiere de un proceso de acreditación. La CA autenticará la solicitud confirmando la validez de la solicitud, la identidad del Firmante/Subscriptor y si el motivo

por el cual el certificado no se encuentra en poder del Firmante/Subscriptor o su representante.

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.

Cuando la solicitud de revocación realice SIN CERTIFICADO el Firmante/Subscriptor o su representante tendrán un período limitado para personarse en la RA y someterse al proceso de acreditación correspondiente. Si finalmente la suspensión no da lugar a la revocación definitiva y el certificado tiene que ser de nuevo activado, el Firmante/Suscriptor recibirá un correo indicando el nuevo estado del certificado.

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias de negocio de AVANSI.

Estos servicios estarán disponibles las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la CA, la CA realizará los mayores esfuerzos para asegurar que estos servicios no se encuentren inaccesibles durante un periodo máximo de 24 horas.

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.

4.4.5.1. Límite del período de revocación

El límite en la decisión de revocar o no un certificado estará estipulado en las Políticas de certificación correspondientes.

4.4.6. Frecuencia de emisión de CRLs

La CA publicará las CRLs con una frecuencia de 24 horas, pudiéndose publicar de manera extraordinaria en cualquier momento en caso de ser aprobado por la Autoridad de Políticas ante cualquier eventualidad que así lo recomiende.

Al mismo tiempo, la CA ofrece el servicio de validación online, basado en el protocolo OCSP (RFC6960), que ofrece el estado en tiempo real.

4.4.7. Requisitos de comprobación de CRLs

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, que podrá descargarse en los siguientes enlaces:

- **http://crl.avansi.com.do/avansisub.crl**
- **http://crl2.avansi.com.do/avansisub.crl**

La CRL's están firmadas por la CA que ha emitido el certificado.

El Tercero que confía deberá comprobar que la lista de revocación es la última emitida ya que pueden encontrarse a la vez varias listas de revocación válidas.

El Tercero que confía deberá asegurarse que la lista de revocación está firmada por la CA que ha emitido el certificado que quiere validar.

La verificación de los validez de los certificado es responsabilidad del tercero y gratuita. No obstante la CA podrá imponer una tarifa por el acceso a la CRL, como se plantea en el punto 2.5.3.

4.4.8. Disponibilidad de comprobación on-line de la revocación

La consulta online estará basada en el protocolo OCSP (RFC6960), que ofrece el estado en tiempo real y accesible mediante la siguiente URL de servicio:

- **http://ocsp.avansi.com.do**

4.5. Procedimientos de Control de Seguridad

4.5.1. Tipos de eventos registrados

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.

4.5.3. Períodos de retención para los Logs de auditoría

La información almacenada se conservará al menos durante 5 años.

4.5.4. Protección de los Logs de auditoría

Los logs de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen y son almacenados en dispositivos ignífugos.

Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la CA. Los dispositivos son manejados en todo momento por personal autorizado.

4.5.5. Procedimientos de backup de los Logs de auditoría

La CA dispone de un procedimiento adecuado de backup descrito en su política de seguridad informática, 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.

La CA tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo.

Adicionalmente se mantiene copia en centro de custodia externo.

4.5.6. Sistema de recogida de información de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de gestión de certificados.

4.5.7. Análisis de vulnerabilidades

La CA realiza periódicamente una revisión de discrepancias en la información de los logs y actividades sospechosas, de acuerdo al procedimiento interno establecido al efecto en las políticas de seguridad informática.

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. Período de retención para el archivo

La información detallada en el apartado **¡Error! No se encuentra el origen de la referencia.** en sus incisos i), k) y l), los certificados, los contratos con los Firmantes/Suscriptores y cualquier información relativa a la identificación y autenticación del Firmante/Suscriptor será conservada durante al menos 10 años.

4.6.3. Protección del archivo

La CA asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas. La CA dispone de un documento de seguridad informática, donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

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. Requerimientos para el sellado de tiempo de los registros

Los registros están fechados con una fuente fiable. La CA dispone de un documento de seguridad informática donde describe la configuración de tiempos de los equipos utilizados en la emisión de certificados.

4.6.6. 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.

El documento de seguridad informática de AVANSI detalla el proceso de cambio de claves de la CA. El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión como se explica en el apartado 4.2.

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.

La CA ha desarrollado un Plan de contingencias para recuperar los sistemas críticos en menos de 48 horas.

Cualquier fallo en la consecución de las metas marcadas por este Plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de AVANSI para implementar dichos procesos.

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

AVANSI reestablecerá los servicios críticos de acuerdo con esta CPS dentro de las 48 horas posteriores a un desastre o emergencia imprevista tomando como base el plan de contingencias y continuidad de negocio existente.

La CA dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descrito en el plan de continuidad de negocio.

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. Informará puntualmente a todos los Firmantes/Suscriptores, empleados, terceros que confían, RA's o CA's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 3 meses.

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) Proveerá de los fondos necesarios para continuar la finalización de las actividades de revocación hasta el límite contratado a fin de satisfacer los 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) Transferirá todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación.

5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL

5.1. Controles de Seguridad Física

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso físico a los servicios críticos y que los riesgos físicos de estos elementos sean minimizados.

La CA tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación certificados ofrece protección frente:

a) Accesos físico no autorizados

b) Desastres naturales

c) Incendios

d) Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)

e) Derrumbamiento de la estructura

f) Inundaciones

g) Robo

h) Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Prestador de Servicios de Certificación

i) Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

5.1.1. Ubicación y construcción

Las instalaciones de la CA están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta, y ubicadas en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas es una jaula de Faraday con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas anti- humedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

5.1.2. Acceso Físico

El acceso físico a las dependencias del Prestador de Servicios de Certificación donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables así como Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación y huella dactilar, gestionado por un sistema informático que mantiene un *log* de entradas y salidas automático.

5.1.3. Alimentación eléctrica y aire acondicionado

Las instalaciones de la CA disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado mediante un grupo electrógeno redundante con depósitos de combustible que pueden ser rellenados desde el exterior.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4. Exposición al agua

Las instalaciones de la CA están ubicadas en una zona de bajo riesgo de inundación y planta semi-elevada con cámara de aire debajo y con detección de humedad.

5.1.5. Protección y prevención de incendios

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

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios.

5.1.6. Sistema de almacenamiento

Cada medio de almacenamiento desmontable (cintas, cartuchos, disquetes, etc.), que contenga información clasificada, está etiquetado con el nivel más alto de clasificación de la información que contenga y permanece solamente al alcance de personal autorizado.

La información con clasificación *Confidencial*, independientemente del dispositivo de almacenamiento, se guarda en armarios ignífugos o bajo llave permanentemente, requiriéndose autorización expresa para su retirada.

5.1.7. Eliminación de residuos

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que los medios usados para almacenar o transmitir la información de carácter sensible como las claves, datos de activación o archivos de la CA serán destruidos, así como que la información que contengan será irrecuperable una vez haya dejado de ser útil.

La información sensible es destruida en la forma más adecuada al soporte que la contenga.

a) **Impresos y papel:** mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

b) **Medios de almacenamiento:** antes de ser desechados o reutilizados deben ser procesados para su borrado, físicamente destruidos o hacer ilegible la información contenida.

5.1.8. Backup remoto

AVANSI utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que es independiente del centro operacional. Se requiere de al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2. Controles Procedimentales

5.2.1. Roles de confianza

Los roles de confianza son los que se describen en las respectivas Políticas de Certificación de forma que se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación. Concretamente:

a) Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

b) Las tareas de Certificación se realizarán por al menos tres personas necesitándose al menos de dos para activar la clave privada de la CA. Estas personas no deben formar parte de las tareas de Sistemas ni de Auditoría.

Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría o Certificación.

5.2.2. Número de personas requeridas por tarea

La CA garantiza al menos dos personas para realizar las tareas que se detallen en las Políticas de Certificación correspondientes.

5.2.3. Identificación y autenticación para cada rol

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

5.2.4. Adecuada separación de funciones

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona sólo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados. El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales, tarjetas de acceso físico y llaves.

5.3. Controles de Seguridad de Personal

5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación.

Todo el personal que realiza tareas calificadas como confiables, lleva al menos dos (2) años trabajando en el centro de producción y tiene contratos laborales fijos. Todo el personal esta cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

La CA se asegurará que el personal de registro o Administradores de RA es personal confiable de la organización o de la entidad delegada para realizar las tareas de registro. El Administrador de RA habrá realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, la CA retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

5.3.2. Procedimiento de comprobación de antecedentes

La CA realizará los esfuerzos que razonablemente estén a su alcance para comprobar los antecedentes del personal que labora en áreas sensibles de la CA.

La CA realizará las investigaciones pertinentes antes de la contratación de cualquier persona.

La CA nunca asignará tareas confiables a personal con menos de una antigüedad de 6 meses.

5.3.3. Requerimientos de formación

El personal encargado de tareas de confianza ha sido formado en los términos que establecen las Políticas de Certificación.

5.3.4. Requerimientos y frecuencia de la actualización de la formación

La CA realizará los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y al menos con una frecuencia anual.

5.3.5. Frecuencia y secuencia de rotación de tareas

La frecuencia y rotación de las tareas será definida en el Manual Administrativo de Gestión del Personal de la CA.

5.3.6. Sanciones por acciones no autorizadas

La CA dispone de un régimen sancionador interno, descrito en su política de seguridad, para su aplicación cuando un empleado realice acciones no autorizadas pudiéndose llegar a su cese.

5.3.7. Requerimientos de contratación de personal

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y la requerimientos operacionales empleados por AVANSI.

Cualquier acción que comprometa la seguridad de los procesos aceptados podrían una vez evaluados dar lugar al cese del contrato laboral. Para los requisitos específicos ver el apartado 5.3.1 y las Políticas de Certificación correspondiente.

5.3.8. Controles sobre el personal contratado

Los controles aplicados al personal contratado serán descritos en el Manual Administrativo de Gestión del Talento de la entidad.

5.3.9. Documentación proporcionada al personal

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar una seguridad razonable y garantizar la confiabilidad y competencia del personal en el adecuado cumplimiento de sus funciones.

AVANSI pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las Políticas y la CPS que rigen dichos procesos.

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

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

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 generación de la clave de las CA's se realiza en un dispositivo módulo criptográfico acreditado FIPS-140-2 L3.

Las claves correspondientes a la CA que emite certificados de servidor seguro fueron creadas en un entorno seguro mediante mecanismos software y bajo control dual.

6.1.2. Generación del par de claves del Firmante/Suscriptor

Las claves del Firmante/Suscriptor pueden ser creadas mediante un dispositivos hardware o software autorizados por la CA o pueden ser creadas por AVANSI en formato software PKCS#12.

Las claves son generadas usando el algoritmo de clave pública RSA. Las claves Tienen una longitud mínima de 2048 bits.

6.1.3. Entrega de la clave pública del Firmante/Suscriptor al emisor del Certificado

El envío de la clave privada a AVANSI para la generación del certificado cuando el circuito así lo requiera, se realiza mediante un formato estándar preferiblemente en formato PKCS#10 o X509 autofirmado.

6.1.4. Entrega de la clave pública de la CA a los Terceros que confían

La certificado de la CA y su fingerprint 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.

6.1.5. Tamaño y período de validez de las claves de la CA

El emisor usará claves basadas en el algoritmo RSA con una longitud mínima de 4096 bits para la CA root, y 2048 bits la CA intermedia.

El periodo de uso de la clave privada de la CA raiz e intermedia es de 30 años.

6.1.6. Tamaño y período de validez de las claves del Firmante/Suscriptor

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

El periodo de uso de la clave pública y privada del Firmante/Suscriptor y la posibilidad de renovación de las mismas se definen en las políticas correspondientes.

En ningún caso, dicho periodo excederá la validez de los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

6.1.7. Requisitos para la generación de claves

Las claves de los Firmantes/Suscriptores pueden ser generadas por ellos mismos en un dispositivo autorizado por AVANSI.

Las claves de las CA´s son generadas en un módulo criptográfico acreditado FIPS-140-2 L3.

6.1.8. 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 de los Firmantes/Subscriptores generadas por CA AVANSI podrán usarse en los términos establecidos por las Políticas de Certificación correspondientes, tal y como se describe el apartado 1.4.8.

6.2. Protección de la Clave Privada

6.2.1. Clave Privada de la CA

La clave privada de firma de la CA es mantenida y usada en un dispositivo criptográfico seguro que cumple los requerimientos FIPS 140-2 L3.

Cuando al clave privada de la CA está fuera del dispositivo esta se mantiene cifrada y partida en diferentes dispositivos. Existe un backup de la clave privada de firma de la CA, que es almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro.

Las copias de backup de la clave privada de firma de la CA están almacenadas de forma segura. Este procedimiento se describe en detalle en las Políticas de seguridad de AVANSI.

6.2.2. Clave Privada del Firmante/Suscriptor

La clave privada del suscriptor se puede almacenar en un dispositivo software o hardware. Cuando se almacene en formato software la CA ofrecerá las instrucciones de configuración adecuada para un uso seguro en las aplicaciones reconocidas.

La CA publicará los dispositivos permitidos para la generación y custodia de las claves en su pagina Web http://www.avansi.com.do, en la sección FAQs > ¿En qué soporte se guarda el certificado digital?

La información respecto al tipo de creación y custodia de claves está incorporada en el propio certificado digital permitiendo a la Tercero que confía actuar en consecuencia.

6.3. Estándares para los Módulos Criptográficos

Los módulos criptográficos empleados son homologados FIPS-140-2 L3.

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

Se requerirá un control múltipersona para la activación de la clave privada de la CA. En el caso de esta CPS se necesitan al menos 2 de 4 personas para la activación de las claves.

6.3.2. Custodia de la clave privada (key escrow)

La CA únicamente almacenará una copia de la clave privada del suscriptor cuando esta se use exclusivamente para cifrado de datos.

6.3.3. Copia de seguridad de la clave privada

La CA realiza una copia de backup de las claves privadas de la CA's que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas.

6.3.4. Archivo de la clave privada

Las claves privadas de las CA’s serán archivadas por un periodo no inferior a 10 años después de la emisión del último certificado.

6.3.5. Introducción de la clave privada en el módulo criptográfico

Existe un documento de ceremonia donde se describe los procesos de generación de la clave privada y el uso del hardware criptográfico.

6.3.6. Método de activación de la clave privada

El acceso a la clave privada del Firmante/Suscriptor se realiza por medio de un PIN que conocerá solamente este que evitará tenerlo por escrito. La clave privada de la CA será activada conforme al apartado 6.3.1.

6.3.7. Método de desactivación de la clave privada

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

La clave privada del Firmante/Suscriptor también quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura.

6.3.8. Método de destrucción de la clave privada

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

Se destruirán físicamente o reinicializarán bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de las CA's de las Jerarquías. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

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. Período de uso para las claves públicas y privadas

Un certificado no debería ser usado después del periodo de validez del mismo aunque el Tercero que confía pueda usarlo para verificar datos históricos teniendo en cuenta que no existirá un servicio de verificación válido para ese certificado.

Para verificar el periodo de uso específicos de las claves ver los apartados 6.1.5 y 6.1.6.

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.

6.5. Ciclo de Vida del Dispositivo Seguro de Almacenamiento de los Datos de Creación de Firma (DSADCF) y del Dispositivo Seguro de Creación de Firma (DSCF).

Los certificados de la CA se almacenan en un dispositivo seguros de creación de firma (DSCF) o en dispositivo seguro de almacén de datos de creación de firma (DSADCF).

El dispositivo DSADCF se entrega en formato PKCS#12 para importarlo en las aplicaciones. El fichero queda en custodia del usuario para su posible recuperación, debiendo guardar los datos de instalación en lugar separado del fichero de claves.

Otro caso de dispositivo software es el empleado en los certificados de servidor seguro donde las claves se generan con los recursos de la aplicación del servidor de páginas donde se va a albergar el certificado.

El dispositivo DSCF se entrega en dispositivo hardware consistente en una tarjeta criptográfica que cumple los requerimientos de acreditación determinados en la legislación vigente o al menos ITSEC E4+.

6.5.1. Dispositivos de Hardware (Smartcard)

La gestión de distribución del soporte la realiza AVANSI directamente quien los distribuye a las autoridades de registro para su entrega personal al suscriptor, junto a la documentación relacionada al dispositivo contratado, entre la que se encuentra el PIN y PUK de acceso a la tarjeta.

El Firmante/Subscriptor utiliza el dispositivo para generar el par de claves y enviar la clave pública a la CA.

La CA envía un certificado de clave pública al suscriptor que es introducido en el dispositivo. El dispositivo es reutilizable y puede mantener de forma segura varios pares de clave.

6.6. Controles de Seguridad Informática

La CA emplea sistemas fiables para ofrecer sus servicios de certificación. Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de AVANSI en los siguientes aspectos:

a) Configuración de seguridad del sistema operativo.

b) Configuración de seguridad de las aplicaciones.

c) Dimensionamiento correcto del sistema.

d) Configuración de Usuarios y permisos.

e) Configuración de eventos de log.

f) Backup y recuperación

g) Configuración antivirus.

h) Requerimientos de tráfico de red.

El documento de seguridad de AVANSI detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

6.6.1. Requerimientos técnicos de seguridad informática específicos

Cada servidor de CA incluirá las siguientes funcionalidades:

a) Control de acceso a los servicios de CA y gestión de privilegios

b) Imposición de separación de tareas para la gestión de privilegios

c) Identificación y autenticación de roles asociados a identidades

d) Archivo del historial del Firmante/Suscriptor y la CA y datos de auditoria

e) Auditoria de eventos relativos a la seguridad

f) Auto-diagnóstico de seguridad relacionado con los servicios de la CA

g) Mecanismos de recuperación de claves y del sistema de CA

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

6.6.2. Valoración de la Seguridad Informática

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad. La seguridad física está garantizada por las instalaciones ya definidas eb el apartado 5.1 y la gestión de personal es manejable debido al reducido número de personas que realizan sus trabajos en el centro de datos de la CA.

6.7. Controles de Seguridad del Ciclo de Vida

6.7.1. Controles de desarrollo del sistema

La CA posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

6.7.2. Controles de gestión de la seguridad

6.7.2.1. Gestión de seguridad

La CA desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad.

La CA exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.7.2.2. Clasificación y gestión de información y bienes

La CA mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de CA AVANSI detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad. Los documentos están catalogados en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL.

6.7.2.3. Operaciones de gestión

La CA dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En el documento de seguridad de AVANSI se desarrolla en detalle el proceso de gestión de incidencias.

La CA dispone de cajas de seguridad ignifugas para el almacenamiento de soportes físicos.

La CA tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

Tratamiento de los soportes y seguridad

a) 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

b) 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

c) 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

d) 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.

6.8. Controles de Seguridad de la Red

6.8.1. Gestión del sistema de acceso

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

CA General

a) Se dispone de controles basados en firewalls de alta disponibilidad.

b) Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.

c) La CA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.

d) La CA dispone de un procedimiento para asegurar que las operaciones se realizan respetando la política de roles.

e) Cada persona tiene asociado su identificador para realizar las operaciones de certificación según su rol.

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

Generación del certificado

g) Las instalaciones de la CA están 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.

h) La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la CA

6.8.2. 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 al sistema de revocaciones.

La revocación se refiere a la pérdida de efectividad de un certificado digital de forma permanente. La revocación se realizará mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de CA.

Estado de la revocación

a) La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

6.8.3. Gestión del ciclo de vida del hardware criptográfico

La CA realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que:

a) La CA se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.

b) El hardware criptográfico esta construido sobre soportes preparados para evitar cualquier manipulación.

c) La CA registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

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

e) La CA realiza pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

f) El dispositivo hardware criptográfico sólo es manipulado por personal confiable.

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

h) La configuración del sistema de la CA así como sus modificaciones y actualizaciones son documentadas y controladas.

i) La CA posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.9. 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.

6.10. Controles de Ingeniería de los Módulos Critpográficos

Todas las operaciones criptográficas de la CA son realizadas en un módulo criptográfico acreditado FIPS-140-2 L3.

7. PERFILES DE CERTIFICADOS 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.

7.1.2. Extensiones del certificado

Las extensiones de los certificados se definen en las Políticas de Certificación correspondientes.

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

El perfil de las CRLs se corresponde con el propuesto en las Políticas de certificación correspondiente. Las CRLs son firmadas por la CA que ha emitido los certificados.

7.2.1. Número de versión, CRL y extensiones

Las CRL y extensiones serán impuestas por las Políticas de Certificación correspondientes.

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 la Declaración de Prácticas de Certificación (CPS).

8.2. Procedimientos de Especificación de Cambios

Cualquier elemento de esta CPS es susceptible de ser modificada. Todos los cambios autorizados sobre las CPS serán inmediatamente publicados en la web de AVANSI.

En la web de AVANSI se mantendrá un histórico con las versiones anteriores de las CPS. 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 CPS estará disponible en formato electrónico en la dirección de Internet: http://politicas.avansi.com.do

8.4. Procedimientos de Aprobación de la CPS

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

ANEXO 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

DSCF - Dispositivo seguro de creación de firma

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

FIPS - *Federal Information Processing Standard Publication*

IETF - *Internet Engineering Task Force*

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

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

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

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

OID - *Object Identifier*. Identificador de objeto

PA - *Policy Authority*. Autoridad de Políticas

PC - Política de Certificación

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

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

PSC - Prestador de Servicios de Certificación

RA - *Registration Authority* Autoridad de Registro

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

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

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

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

ANEXO II: DEFINICIONES

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

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

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

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

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

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

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

CPS – (Certificate Practice Statement) - Conjunto de prácticas adoptadas por una Entidad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.

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

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

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

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

Entidad de Certificación - También conocida como Autoridad de Certificación es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Firmante/Suscriptor y el Tercero que confía, vinculando una determinada clave pública con una persona,

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

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

a) que los datos no han sido modificados (integridad)

b) que la persona que firma los datos es quien dice ser (identificación)

c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)

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

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

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

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

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

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

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

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