

**Normas y Criterios de Auditoría de los Servicios
de Certificación
(ANF AC)**
ANF Autoridad de Certificación

Anexo III

Fecha : 1 de diciembre de 2003

Versión: 1.0

OID : 1.3.6.1.4.1.18332.11.1

Este documento es propiedad de ANF Autoridad de Certificación.

Se autoriza su reproducción y difusión siempre que se reseñe:

- © Copyright ANF Autoridad de Certificación -

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 1 de 66

Normas y Criterios de Auditoría



Sumario

- I. Introducción**
 - a. Presentación.
 - b. Identificación.

- II. Estrategia del Sistema de Auditoría**
 - a. Marco estratégico

- III. Estructura del Sistema de Auditoría**
 - a. Informes de Auditoría
 - b. Frecuencia de las auditorías de gestión
 - c. Monitorizaciones periódicas

- IV. Controles del entorno de ANF AC**
 - a. Ambiente de Control de la EPSC
 - i. Administración de la Política de Certificación y del Manual de Procedimientos de Certificación.
 - ii. Administración de la Seguridad
 - iii. Clasificación y control de activos
 - iv. Seguridad del Personal
 - v. Seguridad física y ambiental
 - vi. Administración de operaciones
 - vii. Administración de accesos al sistema
 - viii. Desarrollo y mantenimiento de los sistemas
 - ix. Administración de la continuidad del negocio
 - x. Comprobación y conformidad
 - xi. Registro de eventos
 - xii. Seguridad criptográfica
 - b. Controles sobre la administración del ciclo de vida de las claves
 - i. Generación de claves de ANF AC
 - ii. Almacenamiento, backup y recuperación de claves de ANF AC
 - iii. Distribución de la clave pública de ANF AC
 - iv. Custodia de las claves de ANF AC
 - v. Utilización de las claves de ANF AC
 - vi. Destrucción de las claves de ANF AC
 - vii. Archivo de las claves de ANF AC
 - viii. Administración del ciclo de vida del hardware criptográfico
 - c. Controles sobre el ciclo de vida del certificado
 - i. Registro del suscriptor
 - ii. Renovación de certificados
 - iii. Re-emisión de claves del certificado
 - iv. Distribución de certificados

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 2 de 66

-
- v. Revocación de certificados
 - vi. Suspensión de certificados
 - vii. Procesamiento de la información del estado de los certificados
 - viii. Administración del ciclo de vida de dispositivos externos de circuitos integrados (Integrated Circuit Cards, en adelante dispositivos).
- d. Controles sobre el estado de la técnica
 - i. Falsificación de Certificados
 - ii. Ataques al Componente TOE

V. Controles del Sistema de ANF AC

- a. Elementos del Sistema
 - i. Interpretación de las definiciones
- b. Requerimientos
- c. Normativa legal

VI. Siglas

VII. Orígenes y objetivos de los principales estándares contemplados en este documento.

VIII. Bibliografía

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 3 de 66

I. Introducción

I.a Presentación.

El presente documento describe las normas y criterios aplicables al Sistema de Auditoría de la Infraestructura de Claves Públicas de **ANF Autoridad de Certificación** (en lo adelante, **ANF AC**), en el marco de su Declaración de Prácticas de Certificación (CPS), y sus Políticas de Certificación (CP), el cual incorporara las siguientes secciones:

- a) Referencias a estándares y experiencias adoptadas internacionalmente. Para este componente cabe acotar que el campo de la auditoría de PKI es relativamente nuevo, siendo escasos los documentos y prácticas internacionales existentes.
- b) Propuesta de estrategia a seguir para la realización de las auditorías de la **ANF AC**, de acuerdo a las directrices trazadas en su CPS, CP y las normas legales vigentes en esta materia.
- b) Definición de los criterios de auditoría. Esta sección detallará los criterios básicos que una **Entidad Prestadora de Servicios de Certificación** (en lo adelante, **EPSC**) debe contemplar para la implementación de un ambiente de control que asegure un adecuado desempeño de sus actividades y en cumplimiento de la Ley. Estos criterios servirán como guía para la evaluación que deberá llevarse a cabo durante las auditorías, tanto internas como externas. Se describirán los objetivos y procedimientos de control, definidos estos últimos como aquellas prácticas recomendadas referidas a aspectos comerciales, operativos, técnicos y jurídicos de esta CA. La CPS, sus Anexos y las CP's que ANF AC ha publicado incluyen los mecanismos que se utilizan para implementar estos objetivos y procedimientos de control, que se definen en función de una previa evaluación de riesgos.
- c) Estructura de las auditorías. En esta sección se proponen los aspectos relativos a la frecuencia de las auditorías, la obligación de publicación y los informes de conclusiones de las evaluaciones realizadas. Con relación a las normas de seguridad respecto de los sistemas de auditoría, se citan las normas internacionales, los estándares y las prácticas en uso aplicables a cada procedimiento de control. De igual forma, se incluye los objetivos de control, el detalle de los procedimientos de control y las referencias a normas de seguridad, como una guía para la realización de auditorías.

Este documento sirve como base tanto para la elaboración de las auditorías por parte de **ANF AC** como para el proceso de contratación de las firmas de auditores externos, cuando sea necesario, para la realización de las auditorías de gestión.

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 4 de 66

1.b Identificación.

Nombre del documento	Normas y Criterios de Auditoría de los Servicios de Certificación
Versión	1.0
Autor	<i>Florencio Díaz Vilches</i>
Referencia del documento / OID	1.3.6.1.4.1.18332.11.1
Fecha de emisión	1 de diciembre de 2002
Fecha de expiración	No es aplicable
Localización URL	http://www.anf.es/AC/documentos/

El prefijo del OID de este documento es 1.3.6.1.4.1.18332.11.

Cualquier modificación que esta Autoridad de Certificación realice sobre este documento, conllevará un cambio de versión y del identificador de objeto (OID).

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 5 de 66

II. Estrategia del Sistema de Auditoria

II.a. Marco Estratégico.

II.a.1 Función de la auditoria en el marco de la Ley.

La practica totalidad de países avanzados del mundo han desarrollado legislaciones específicas que regulan el funcionamiento de los servicios de certificación digital, así como la recogida, el almacenamiento informatizado y posterior uso de los datos de las personas físicas.

La auditoria tiene asignada una función de vigilancia y control de los servicios desarrollados por ANF AC, y en especial la adecuación de su actividad al marco legal según cada país en los que opera.

II.a.2 Función de la auditoria en el marco de las obligaciones asumidas por ANF AC es su CPS, Anexos y CP's.

En relación al sistema de auditoría, la persona o personas que ejercen la función de auditor asumen las siguientes responsabilidades:

- Determinar el sistema de inspección y auditoria sobre los elementos contemplados en su sistema PKI, incluyendo las modalidades de difusión de los informes de auditoria y los requisitos de habilitación de entidades para efectuar auditorias y los criterios y estándares de auditoria mínimos que deberán cubrir;
- Efectuar las inspecciones y auditorias previstas en la Ley, su Reglamento de Aplicación y las normas de la propia EPSC como su CPS, Anexos y CP's;
- Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas en los dictámenes de auditoria sobre los elementos controlados, para determinar, en su caso, si ha adoptado las acciones correctivas correspondientes;
- Ejercer la facultad de auditoria e inspección sobre los sistemas y procedimientos que emplea la infraestructura de la EPSC. Dicha facultad de inspección comprende tanto la inspección ordinaria como la extraordinaria. La inspección ordinaria consiste en la facultad de practicar auditorias de gestión periódicas a las instalaciones y sistemas de la EPSC, así como realizar un monitoreo permanente sobre el desarrollo de la actividad. La inspección extraordinaria será practicada siempre que se produzca una reclamación o denuncia sobre la prestación de alguno de los servicios o situaciones de posible incumplimiento detectadas, por sí o por terceros;
- Fijar los criterios que deben cumplir los terceros contratados para colaborar con las inspecciones y auditorias;
- Notificar a la Junta Rectora de la PKI y Publicar en el Registro de Auditorias de la Web institucional de ANF AC localizada en la URL <http://www.anf.es/AC/documentación/>, el resultado de la evaluación obtenida en la última auditoria e inspección realizada;
- Solicitar del personal empleado o colaborador de esta EPSC, informes y datos que sean adecuados a la finalidad legítima, en los procesos de auditoria establecidos por la legislación aplicable y a su reglamentación;
- Comprobar que la CPS, los Anexos y las CP's aplicadas con concordantes con todos los aspectos relativos a este documento de auditoria e inspección. Así

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 6 de 66

-
- mismo, verificar la vigencia es documentación en base al resultado de las evaluaciones obtenidas en la última auditoria e inspección realizada;
- Requerir que sea revocado el certificado o los certificados de la CA si se determina, en virtud de la auditoria realizada, que los procedimientos de guarda y custodia han dejado de ser seguros y se sospecha sobre la integridad de los mismos .
Establecer si la tecnología empleada por ANF AC, mantiene las condiciones de seguridad y operativas requeridas por su reglamento y la legislación vigente. Así como a ver realizado las actualizaciones tecnológicas que pudieran haberse producido;
 - Controles de monitorización de procesos y análisis de Log. Se agrupan en la categoría de procesos ordinarios de auditoria e inspección permanente al que esta sometida esta EPSC;
 - Las actividades mencionadas, si bien poseen un fuerte componente tecnológico, involucran también aspectos legales, de verificación de cumplimiento del marco normativo existente y de revisión de las prácticas y políticas de certificación y otros manuales técnicos. Por todo ello, las auditorias e inspecciones serán realizadas por personal titulado en las áreas de informática o telecomunicaciones y Derecho.

Audidores Externos: Serán responsables de efectuar las **auditorias periódicas**, a petición de ANF AC.

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 7 de 66

III. Estructura del Sistema de Auditoria

La auditoría es un proceso formal y necesario para las EPSC, que tiene por objeto de verificar el cumplimiento oportuno de las normas, políticas y procedimientos relacionados con la prestación de sus servicios. En particular la auditoría de sistemas se orienta a la revisión del cumplimiento de las normas, políticas y procedimientos del entorno informático de la EPSC.

III.a Informes de Auditoría.

Una vez que ha culminado la revisión de auditoria, se procede a la elaboración de un documento final o informe de auditoria que contiene el dictamen y el detalle de las tareas realizadas.

Dicho informe debe reflejar las observaciones, debilidades de control, acciones propuestas de mejoramiento, plazos sugeridos para su realización, responsables y personas involucradas, todo lo cual servirá de base para el dictamen final.

Debe estar dirigido a ANF AC y remitirse una copia a la Junta Rectora de la PKI

Los informes deben cumplir con las siguientes condiciones:

- Ser veraz, de manera tal que permita el arribo a conclusiones con la certeza de que los datos son reales y de fuentes confiables, plenamente identificadas.
- Estar documentado formalmente.
- Mostrar las observaciones encontradas, clasificadas por orden de importancia o por el impacto negativo que puede tener sobre la prestación de los servicios de certificación. Si se considera conveniente puede señalarse el riesgo asociado a las observaciones que se formulan.
- Enumerar recomendaciones para cada observación.

El dictamen contenido en el informe, que refleja las conclusiones del trabajo de auditoria, puede ser:

Favorable: se interpretará que ANF AC posee un ambiente de control que permite inferir que se trata de una entidad razonablemente confiable, en cuanto a sus procesos de administración del ciclo de vida de los certificados y al cumplimiento de las disposiciones vigentes aplicables.

Con observaciones: debe de interpretarse que ANF AC debe de corregir algunos aspectos concretos, los cuales, sin ser graves ni afectar a la seguridad de los servicios que presta, si que impiden la emisión de un dictamen favorable. Como parte del proceso de auditoria, se efectuarán revisiones de seguimiento a fin de determinar la subsanación de las incidencias detectadas y se establecerá un plazo para la rectificación de los problemas encontrados.

Desfavorable: se interpretará que ANF AC no posee un ambiente de control que permita ejercer sus actividades como EPSC.

ANF AC asume la obligación de publicar en su sitio de Internet los informes de auditoria, cualquiera que sea su condición. URL de localización <http://www.anf.es/AC/documentos/>

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 8 de 66

III.b Frecuencia de las auditorías de gestión.

Las auditorías de gestión se efectuarán como mínimo una vez por año, o de acuerdo a lo dispuesto en cada Política de Certificación según los certificados emitidos por ANF AC en cada momento.

III.c Monitorizaciones periódicas.

Las monitorizaciones periódicas que deben de efectuarse se referirán entre otros aspectos:

- A la verificación de la publicación de todas las novedades y actualizaciones de la documentación de esta EPSC.
- A la constatación de la accesibilidad de las Practicas y de las Políticas de Certificación.
- A la verificación de la prestación continua de la publicación de los Certificados Emitidos y Revocados.
- A la verificación de la prestación continua de la publicación de los Sellos de Tiempo emitidos por ANF AC.
- A la verificación de la sincronización horaria de los equipos dedicados a la estampación de Sellos de Tiempo.
- A la verificación de la prestación continua de los distintos servidores que componen la infraestructura distribuida de servicios de firma electrónica.
- A la verificación en la publicación de todo el software utilizado por los usuarios de esta EPSC, especialmente de las novedades y actualizaciones que se hayan producido.
- Al seguimiento de las quejas o denuncias de los usuarios y suscriptores de certificados, y de los terceros de confianza, que sin reunir en forma independiente las condiciones y entidad suficiente para provocar la realización de inspecciones, puedan motivarlas al analizar su frecuencia o periodicidad o reiteración.

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 9 de 66

IV. Controles del entorno de ANF AC

Los objetivos y procedimientos de control que se describirán a continuación representan los criterios mínimos a los que se deberá ajustar ANF AC para ejercer su actividad como entidad prestadora de servicios de certificación.

Estos criterios están basados en el estándar ANSX9.79:2001 de la American National Standard Institute (ANSI), con las adaptaciones relativas a las particularidades de la directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica y a las normas técnicas cuyos números de referencia hayan sido publicados en el «Diario Oficial de la Unión Europea», así como a las obligaciones asumidas por ANF AC en sus Prácticas y Políticas de Certificación.

Los mecanismos, procesos y objetivos de control referenciados se orientan a evaluar y establecer la situación de ANF AC con relación a su entorno tecnológico para la gestión del ciclo de vida de los certificados digitales y de restantes servicios de certificación que se encuentra habilitada para prestar.

Los objetivos de control han sido agrupados en cuatro secciones. En todas ellas el auditor debe realizar aquellas pruebas sustantivas y de cumplimiento que le permitan verificar la existencia, el cumplimiento y la eficacia de los procedimientos de control implementados. Debe de revisar las prácticas, las políticas y los manuales de publicados por ANF AC, y asegurarse que los mismos son conocidos y aplicados por el personal correspondiente. Las pruebas podrán incluir revisiones de la documentación, utilización de software específico de auditoría, de programas utilitarios adecuados para la revisión, así como inspecciones oculares y entrevistas al personal y todo otro procedimiento que juzgue conveniente.

La actual legislación en materia de Firma Electrónica responsabiliza a los prestadores de servicios de certificación que expidan certificados reconocidos, sobre el empleo de sistemas y productos que estén debidamente protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte (Ley 59/2003 Art. 20.e y e). De especial relevancia es la sección "IV.d Controles sobre el estado de la técnica", en la que el auditor debe de verificar que los dispositivos homologados por ANF AC tienen incorporadas medidas de salvaguarda suficientes contra los ataques que se han producido, con resultados positivos, sobre instrumentos comúnmente utilizados en Sistemas PKI, así como las medidas de seguridad establecidas Protection Profile CWA-14167-2

A continuación se presentan los criterios mínimos de cada sección, los cuales deben de interpretarse como una guía, respecto a los objetivos y procedimientos de control que deben estar implementados por ANF AC. Resulta esencial que el auditor utilice su juicio profesional para determinar la naturaleza, el alcance y la oportunidad de las pruebas de auditoría a realizar, con el fin de emitir una opinión sobre el ambiente de control interno y el cumplimiento del marco normativo aplicable.

IV.a Ambiente de Control de la EPSC

i. Administración de la Política de Certificación y del Manual de Procedimientos de Certificación

Objetivos de control. ANF AC debe de mantener controles para proveer un nivel razonable de seguridad sobre la efectividad de la administración de la Declaración

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 10 de 66

de Prácticas de Certificación y de las Políticas de Certificación (CP's), vinculadas a los certificados que emite.

Procedimientos de control	Referencias
Autoridad de Administración de políticas ¹	
La organización posee un grupo de administración con autoridad final y responsabilidad para definir y aprobar las CPS y CP's. Cambios en el OID.	RFC 2527 4.8.1 X.9.79 A
Existe un órgano de control de la Política de Certificación con autoridad final y responsabilidad para definir y aprobar la CPS	CARAT B.2
El órgano de control de la PKI ha efectuado una evaluación de los riesgos de la actividad de la EPSC y ha determinado los requerimientos de seguridad y procedimientos operativos a ser incluidos en la CPS y CP's aplicables, respecto a los siguientes aspectos: a) Controles del ambiente de ANF AC. b) Controles de administración del ciclo de vida de las claves. c) Controles sobre el ciclo de vida del certificado.	CARAT B.2.1
Administración de las Prácticas de Certificación	
La CPS es aprobada y modificada de acuerdo con un procedimiento de revisión predeterminado, incluyendo la definición de responsabilidades para su mantenimiento	X.9.79 7.2
ANF AC pone su CPS, a disposición de todos sus suscriptores y usuarios de certificados, y terceros de confianza.	RFC 2527 4.8.2 X.9.79 A
Las revisiones de la CPS son puestas a disposición de todos los suscriptores y usuarios de certificados	RFC 2527 4.8.1 X.9.79 A
La CPS y las CP's se contemplan las especificaciones establecidas según las orientaciones internacionales en la materia.	RFC 2527
Administración de las Políticas de Certificación	
Cada CP es aprobada y modificada de acuerdo con un procedimiento de revisión predeterminado, incluyendo la definición de responsabilidades para su mantenimiento	X.9.79 7.1
Existe un procedimiento de revisión definido para asegurar que la CP es soportada por la CPS de ANF AC.	X.9.79 7.2
ANF AC pone a disposición de sus suscriptores y terceros confianza las CP's que soporta.	RFC 2527 4.8.2 X.9.79 A
Las revisiones a las CP's soportadas por ANF AC son puestas a disposición de los suscriptores y usuarios.	RFC 2527 4.8.1 X.9.79 A

¹ Comité interno de ANF AC, reconocido dentro de la CPS como Junta Rectora de la PKI.

ii. Administración de Seguridad

Objetivos de control. ANF AC debe mantener controles que permitan asegurar razonablemente que:

- a) Existen normas claras de la gerencia y un adecuado soporte a la seguridad de la información;
- b) La seguridad de la información es administrada adecuadamente dentro de la organización;
- c) Se mantiene adecuadamente la seguridad de los servicios, sistemas y activos de la EPSC accedidos por terceros; y,
- d) Se mantiene el mismo nivel de seguridad de la información cuando una o varias funciones de la EPSC son subcontratadas a otra organización.

Procedimientos de control	Referencias
Política de Seguridad de la Información	
La dirección aprueba un documento referido a la Política de Seguridad de la información (denominado "Plan de Seguridad"), el cual es publicado y puesto en conocimiento de todo el personal.	ISO 17799 3.1.1
La Política de Seguridad contiene la definición de la seguridad de la información, sus objetivos principales y alcance, haciendo referencia a su importancia como un mecanismo que habilita el uso compartido de la información.	ISO 17799 3.1.1
La Política de Seguridad define el rol del Responsable de la Información y de los Jefes de Seguridad, como soporte de los objetivos y principios de la seguridad de la información.	ISO 17799 3.1.1
La Política de Seguridad contiene una explicación de los principios, estándares y requerimientos de seguridad de particular importancia para la organización, incluyendo, como mínimo: <ul style="list-style-type: none"> a) Adecuación a las disposiciones legales. b) Requerimientos de capacitación y formación en el tema. c) Prevención y detección de virus y software malicioso. d) Continuidad de la administración de los negocios. e) Consecuencias de violaciones a la Política de Seguridad. 	ISO 17799 3.1.1
La Política de Seguridad contiene referencias a la documentación de soporte.	ISO 17799 3.1.1
Existe un proceso de revisión definido, incluyendo frecuencias y responsabilidades, para el mantenimiento del Plan de Seguridad.	ISO 17799 3.1.2
Infraestructura de seguridad de la información	

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 12 de 66

Existe un responsable de seguridad de la información del más alto nivel que asegura que existan claras normas y administración de soporte para las iniciativas de seguridad.	ISO 17799 4.1.1
Existe un responsable de administración de seguridad que coordina la implementación de las medidas de seguridad de la información.	ISO 17799 4.1.2
Las responsabilidades por la protección de los activos y por la implementación de procesos específicos de seguridad se encuentran claramente definidas.	ISO 17799 4.1.3
Existe y se cumple un procedimiento de autorización para los nuevos servicios de procesamiento de información.	ISO 17799 4.1.4
Seguridad de acceso de terceros	
Existen y se cumplen procedimientos de control de acceso físico y lógico a los servicios y sistemas de ANF AC por parte de terceros, incluyendo personal de empresas contratadas y equipo propio.	ISO 17799 4.2
En caso de existir una necesidad comercial para que ANF AC autorice el acceso de terceros a sus servicios y sistemas, se efectúa una evaluación de riesgos para determinar sus implicaciones para la seguridad y los controles específicos requeridos.	ISO 17799 4.2.1.1 ISO 17799 4.2.1.2
Los acuerdos referidos al acceso de terceros a los servicios y sistemas de ANF AC están basados en un contrato formal que contiene todos los requerimientos de seguridad necesarios.	ISO 17799 4.2.2
Subcontratación	
En caso de que ANF AC subcontrate la administración y el control de uno o varios de sus sistemas de información, redes y/o entornos de oficina, los requerimientos de seguridad se incluyen en un contrato acordado por las partes.	ISO 17799 4.3.1
ANF AC puede optar por delegar una parte de sus roles y de sus respectivas funciones, siendo igualmente responsable final por el cumplimiento de las funciones definidas y por la definición y mantenimiento de su CPS. Esta particularidad debe de estar definida en los documentos aplicables.	X 9.79 6

iii. Clasificación y control de activos

Objetivos de control. ANF AC tiene que mantener controles que provean de razonable seguridad a sus activos y a la información que posee registrada, y que todo ello recibe un adecuado nivel de protección

Procedimientos de control	Referencias
Clasificación y Administración de Activos	

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 13 de 66

Se designan propietarios de cada uno de los principales activos de ANF AC y se asignan responsabilidades para el mantenimiento de controles apropiados.	ISO 17799 5.1.1
Se mantienen inventarios de los principales activos de ANF AC	ISO 17799 5.1.1
ANF AC ha implementado un sistema de clasificación de la información con controles de protección asociados, teniendo en cuenta las necesidades del negocio para compartir o restringir el acceso a la información, así como el impacto en el negocio de dichas necesidades.	ISO 17799 5.2.1
Se definen procedimientos para asegurar que el rotulado y manejo de la información se efectúa de acuerdo con el esquema de clasificación de la información de ANF AC.	ISO 17799 5.2.2

iv. Seguridad del Personal

Objetivos de control. ANF AC debe mantener controles para proveer un nivel razonable de seguridad de que las prácticas de contratación y control del personal, respaldan y aumentan la confiabilidad de sus operaciones.

Procedimientos de control	Referencias
Seguridad del personal	
Los roles y responsabilidades de seguridad especificados en la política de seguridad de ANF AC, se documentan en las descripciones de las tareas.	ISO 17799 6.1.1
Se efectúan controles de verificación de personal permanente al momento de su contratación. Las políticas y procedimientos de ANF AC especifican los controles de antecedentes requeridos para: <ul style="list-style-type: none"> a) El personal que desempeña roles confiables. b) Otro personal, incluyendo el de limpieza. 	ISO 17799 6.1.2, RFC 25274.5.3.2 RFC 25274.5.3.2 X9.79 A
ANF AC ha implementado un sistema de clasificación de la información con controles de protección asociados, teniendo en cuenta las necesidades del negocio para compartir o restringir el acceso a la información, así como el impacto en el negocio de dichas necesidades.	ISO 17799 5.2.1
Los empleados firman un acuerdo de confidencialidad como parte de los términos y condiciones de su incorporación..	ISO 17799 6.1.3
Los controles sobre el personal contratado incluyen: <ul style="list-style-type: none"> a) La evaluación de la confiabilidad del personal a contratar; b) Los requerimientos contractuales que incluyan indemnizaciones por daños causados por acciones del personal contratado y, c) El derecho a la auditoría y el monitoreo del personal contratado. 	RFC 2527 4.5.3.7 X9.79 A

<p>Todos los empleados de la organización, y de ser necesario, los terceros ajenos a la Entidad de Certificación, reciben capacitación adecuada sobre sus políticas y procedimientos.</p> <p>Las políticas y procedimientos de la ANF AC especifican:</p> <p>a) Los requerimientos y procedimientos de entrenamiento y capacitación para cada rol; y,</p> <p>b) La frecuencia y duración de dichas actividades.</p>	<p>ISO 17799 6.2.1, RFC 2527 4.5.3.4 RFC 2527 4.5.3.5 X9.79 A</p>
<p>Se efectúan revisiones periódicas para verificar que se mantienen las condiciones de confianza del personal involucrado en actividades relacionadas a administración de claves y certificados.</p>	
<p>Existe y se cumple un proceso disciplinario formal para los empleados que han violado políticas y procedimientos de seguridad de la organización. Los procedimientos de ANF AC especifican las sanciones para el personal por acciones o usos no autorizados de los sistemas y de las atribuciones del cargo.</p>	<p>ISO 17799 6.3.5 RFC 2527 4.5.3.6 X9.79 A</p>
<p>Se toman acciones apropiadas y oportunas cuando un empleado deja de desempeñarse en la organización, de manera que los controles internos y de seguridad no se vean perjudicados por dicha circunstancia.</p>	

v. Seguridad Física y Ambiental

Objetivos de control. ANF AC tiene que mantener controles que permitan asegurar razonablemente:

- a) El acceso físico a los servicios se limita al personal autorizado, y dichos servicios son protegidos de riesgos ambientales;
- b) Se previenen las pérdidas, daños o vulneración de activos y las interrupciones en las actividades del negocio; y,
- c) Se previene la vulneración o robo de la información y de servicios de procesamiento de la información.

Procedimientos de control	Referencias
Seguridad física de los servicios de certificación	
Se obtiene protección física a través de la creación de parámetros de seguridad definidos alrededor de las instalaciones (por ejemplo: barreras físicas) y de los servicios de ANF AC.	ISO 17799 7.1.1
El perímetro del edificio o de las instalaciones de la Entidad de Certificación se encuentra físicamente aislado (por ejemplo: no deberían existir brechas en el perímetro, que permitieran rupturas de acceso).	ISO 17799 7.1.1

Existe un área de recepción u otros medios de control de acceso físico que restringen el acceso al edificio o instalaciones de ANF AC únicamente al personal autorizado.	ISO 17799 7.1.1
Se establecen adecuadas barreras físicas a fin de prevenir accesos no autorizados.	ISO 17799 7.1.1
Todas las salidas de emergencia en los perímetros de seguridad alrededor de los servicios de ANF AC poseen señales de alarma.	ISO 17799 7.1.1
Se instalan y prueban regularmente sistemas de detección de intrusos para cubrir todas las puertas externas del edificio de ANF AC y de las instalaciones informáticas.	ISO 17799 7.1.3
Las instalaciones de ANF AC activan sus alarmas cuando se retira el personal.	ISO 17799 7.1.3
Las áreas de producción y en general todas las instalaciones informáticas de ANF AC se encuentran físicamente bajo llave.	ISO 17799 7.1.4
No se autorizan tareas no supervisadas en las instalaciones seguras de ANF AC tanto por razones de seguridad como por prevención de actividades maliciosas.	ISO 17799 7.1.4
Se exige que todo el personal que utilice identificaciones visibles y que denuncie a toda persona que no cumpla con este requisito; caso de autorizarse la realización de tareas sin estar supervisadas permanentemente por el personal de control.	ISO 17799 7.1.2
El acceso a las instalaciones de ANF AC se controla ISO 17799 7.1.2 y restringe a personas autorizadas mediante el uso de controles de autenticación.	ISO 17799 7.1.2
Todo el personal que ingresa o se retira de los servicios de ANF AC debe ser registrado (por ej.: se mantiene un registro seguro de los accesos)	
Las visitas al edificio o a las instalaciones son supervisadas, y se registra la fecha y hora de su ingreso.	ISO 17799 7.1.2
El personal ajeno a la Entidad de Certificación que preste servicios de apoyo puede ingresar a las instalaciones de ANF AC únicamente cuando se solicite su presencia y siempre que dicho acceso sea autorizado y monitoreado.	ISO 17799 7.1.4
Los perfiles de acceso a las instalaciones de ANF AC son revisados y actualizados regularmente.	ISO 17799 7.1.2
Seguridad física del equipamiento	

El equipamiento se encuentra situado y protegido de manera tal de reducir los riesgos de amenazas ambientales y de posibilidades de accesos no autorizados.	ISO 17799 7.2.1 RFC 2527 4.5.1.1, 4.5.1.4 y 4.5.1.5 X9.79 A
El equipamiento se encuentra protegido de fallas energéticas y de otras anomalías en el servicio eléctrico.	ISO 17799 7.2.2 RFC 2527 4.5.1.3 X9.79 A
El cableado de alimentación eléctrica y de telecomunicaciones que transporte datos o soporta servicios de ANF AC se encuentra protegido de interceptaciones o daños.	RFC 2527 7.2.3 X9.79 A
Se sigue un cronograma de mantenimiento del equipamiento, de acuerdo con las instrucciones del fabricante y/o con otros procedimientos documentados que aseguren su continua disponibilidad e integridad.	RFC 2527 7.2.4 X9.79 A
Previo a su destrucción o reutilización, todos los ítems del equipamiento que contienen medios de almacenamiento (por ejemplo: discos rígidos) son revisados con el fin de determinar si contienen algún dato sensible. Los dispositivos de almacenamiento que contienen información sensible son físicamente destruidos o sobrescritos, previo a su reutilización.	ISO 17799 7.2.6 RFC 2527 4.5.1.7 X9.79 A
Seguridad física del equipamiento	
La información sensible o crítica de los negocios es guardada bajo llave cuando no es utilizada y cuando las instalaciones de ANF AC se encuentran vacías.	ISO 17799 7.3.1
Los ordenadores personales y estaciones de trabajo no se dejan encendidas o activadas cuando sus responsables están ausentes y son protegidas por llaves, claves u otros mecanismos de control (por ejemplo = SmartCard)	ISO 17799 7.3.1
El equipamiento, la información y el software que pertenecen a la organización no pueden trasladarse fuera de ella sin autorización.	ISO 17799 7.3.2

vi. Administración de operaciones

Objetivos de control. ANF AC tiene que mantener controles que aseguren razonablemente que:

- a) Se mantiene un correcto y seguro funcionamiento de sus servicios de procesamiento de información;
- b) Se minimizan los riesgos de fallas en los sistemas;
- c) La integridad de los sistemas y datos de ANF AC se encuentra protegida contra virus y software malicioso;
- d) Los daños ocasionados por incidentes de seguridad y funcionamiento deficiente son minimizados a través del uso de reportes de incidentes y procedimientos de respuesta, y
- e) Los medios y soportes son administrados en forma segura, para protegerlos de daños, robo y accesos no autorizados.

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 17 de 66

Procedimientos de control	Referencias
Procedimientos operativos y responsabilidades	
Se documentan y mantienen actualizados los procedimientos operativos de ANF AC.	ISO 17799 8.1.1
Se definen responsabilidades y procedimientos formales de administración para controlar todos los cambios al equipamiento, al software y a los procedimientos operativos de ANF AC.	ISO 17799 8.1.2
Las funciones y áreas de responsabilidad son diferenciadas de manera de reducir las posibilidades de modificaciones no autorizadas o uso indebido de la información o de los servicios.	ISO 17799 8.1.4
Los servicios de desarrollo y prueba se encuentran separados de los operativos.	ISO 17799 8.1.5
Previo a la utilización de servicios externos, se identifican los riesgos y se acuerdan controles apropiados con el contratista, incorporándolos a los contratos.	ISO 17799 8.1.6
Planificación y aceptación de los sistemas	
Se monitorean las demandas de capacidad de procesamiento y almacenamiento, y se efectúan proyecciones de futuros requerimientos para asegurar que se mantienen disponibles las capacidades adecuadas.	ISO 17799 8.2.1
Se establecen criterios de aceptación de nuevos sistemas y aplicaciones informáticas, actualizaciones y nuevas versiones y se establecen pruebas adecuadas como paso previo a dicha aceptación.	ISO 17799 8.2.2
Protección contra virus y software malicioso	
Se implementan controles de detección y prevención para protección ante virus y software malicioso y se establecen procedimientos para concienciar a los empleados, suscriptores y resto de usuarios del sistema.	ISO 17799 8.3.1
Reporte y respuesta ante incidentes	
Existe, y se cumple, un procedimiento formal de reporte de incidentes, junto a un procedimiento de respuesta, estableciendo las acciones a desarrollar después de recibirse el reporte.	ISO 17799 6.3.1
Se exige a los usuarios de los sistemas de ANF AC que reporten las debilidades de seguridad observadas, sospechadas, o que pudieran amenazar los sistemas o servicios.	ISO 17799 6.3.2

Existen y se cumplen procedimientos para reportar el funcionamiento erróneo del software.	ISO 17799 6.3.3
Existen y se cumplen procedimientos para asegurar que se reportan las fallas y se toman acciones correctivas.	ISO 17799 8.4.3
Los tipos, volúmenes y costos de los incidentes y fallas son cuantificados, monitoreados e informados.	ISO 17799 6.3.4
Existen, y se cumplen, los procedimientos y las responsabilidades de administración de incidentes, para asegurar una rápida, efectiva y ordenada respuesta a las fallas de seguridad.	ISO 17799 8.1.3
Reporte y respuesta ante incidentes	
Los procedimientos de administración de medios de almacenamiento móviles requieren: a) En caso de no volver a utilizarse, los contenidos previos de cualquier medio o soporte reutilizable que deban eliminarse de la organización, deben ser borrados. b) Se requiere autorización para todos los medios que se transfieran de la organización y se conserva un registro de auditoría de los mismos. c) Todos los medios se almacenan en un entorno seguro de acuerdo con las especificaciones del fabricante.	ISO 17799 8.6.1
Se desechan en forma segura los medios y soportes cuando no son vueltos a utilizar.	ISO 17799 8.6.2 RFC 2527 4.5.1.7 X9.79 A
Se siguen y cumplen procedimientos para el manejo y almacenamiento de la información a fin de protegerla de la revelación no autorizada o del uso indebido.	ISO 17799 8.6.3
La documentación del sistema es protegida de accesos no autorizados.	ISO 17799 8.6.4

vii. Administración de accesos al sistema

Objetivos de control. ANF AC tienen que mantener controles que permitan asegurar con un nivel razonable de certeza, que el acceso a sus sistemas se encuentra limitado sólo a personas debidamente autorizadas.

Procedimientos de control	Referencias
Administración de accesos del usuario	

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 19 de 66

Los requerimientos del servicio para el control de acceso se definen y documentan en un Plan de Seguridad "control de acceso" que incluye al menos: a) Roles y sus correspondientes perfiles de acceso. b) Procesos de identificación de cada usuario. c) Separación de funciones.	ISO 17799 9.1.1 RFC 2527 4.5.2 y 4.6.5 X9.79 A
Existe un procedimiento formal de registro y baja de usuarios para permitir el acceso a los servicios y sistemas de información.	ISO 17799 9.2.1
Se restringe y controla la asignación y utilización de privilegios.	ISO 17799 9.2.2
La asignación de palabras clave (passwords), en aquellos procedimientos en los que no se utilice el sistema SmartCard (PIN administrado por el propio usuario), se controla a través de un proceso de administración formal.	ISO 17799 9.2.3
Los derechos de acceso de los usuarios se revisan a intervalos regulares.	ISO 17799 9.2.4
Se exige a los usuarios el cumplimiento de políticas y procedimientos definidos para la selección y utilización de palabras clave.	ISO 17799 9.3.1
Se exige a los usuarios asegurar que sus equipos poseen adecuada protección cuando no están siendo utilizados por ellos.	ISO 17799 9.3.2
Controles de acceso de red	
Se provee acceso directo a los usuarios únicamente para los servicios para los que han sido específicamente autorizados.	ISO 17799 9.4.1
Se controla la trazabilidad desde la terminal del usuario hasta los servicios	ISO 17799 9.4.2
En aquellos procesos que esta permitido el acceso de usuarios remotos, se exige autenticación.	ISO 17799 9.4.3
Las conexiones a sistemas remotos se encuentran autenticadas.	ISO 17799 9.4.4
Se controla en forma segura el acceso a los puertos ("ports") de diagnóstico.	ISO 17799 9.4.5

Se establecen controles (ej.: firewalls) a fin de proteger los dominios de la red interna de ANF AC respecto de aquellos dominios de red accesibles por terceros.	ISO 17799 9.4.6
Se establecen controles para limitar el acceso a ciertos servicios disponibles (por ejemplo: HTTP, SOAP, FTP, LDAP, etc.) a determinados grupos de usuarios, de acuerdo a las políticas de control de acceso de ANF AC.	ISO 17799 9.4.7 RFC 2527 4.6.7 X9.79 A
Se establecen controles de trazabilidad para asegurar que las conexiones y flujos de información cumplan con la política de control de acceso de las aplicaciones de la organización.	ISO 17799 9.4.8 RFC 2527 4.6.7 X9.79 A
Los atributos de seguridad de los servicios de red utilizados por la organización son documentados por ANF AC.	ISO 17799 9.4.9 RFC 2527 4.6.7 X9.79 A
Se utilizan identificaciones automáticas de terminales para autenticar las conexiones a ubicaciones específicas del sistema.	ISO 17799 9.5.1
El acceso a los sistemas de ANF AC utiliza un sistema seguro.	ISO 17799 9.5.2
Todos los usuarios tienen una identificación única para su uso personal y exclusivo.	ISO 17799 9.5.3
La utilización de programas está restringida y controlada.	ISO 17799 9.5.5
Previa evaluación de riesgos, y en caso de ser necesario, se realiza un seguimiento de los usuarios que podrían ser objeto de extorsión.	ISO 17799 9.5.6
Las terminales inactivas conectadas a los sistemas de ANF AC se bloquean después de un período previsto de inactividad para prevenir acceso por personal no autorizado.	ISO 17799 9.5.7
Se establecen restricciones en los horarios de acceso para proveer seguridad adicional para aplicaciones de alto riesgo.	ISO 17799 9.5.8
Administración de accesos del usuario	
Se restringe el acceso a la información y a las funciones de las aplicaciones del sistema, de acuerdo con la política de control de acceso.	ISO 17799 9.6.1
Los sistemas sensibles requieren un entorno especializado y aislado.	ISO 17799 9.6.2

viii. Desarrollo y mantenimiento de los sistemas

Objetivos de control. ANF AC tiene que mantener controles que permitan asegurar razonablemente que el desarrollo de los sistemas y las actividades de mantenimiento se encuentran debidamente autorizados a fin de conservar la integridad de sus sistemas.

Procedimientos de control	Referencias
Desarrollo y mantenimiento de los sistemas	
Los requerimientos del servicio para nuevos sistemas, o las mejoras a los sistemas existentes, especifican los requerimientos de control.	ISO 17799 10.1.1
Existen y se cumplen procedimientos de control de cambios para la implementación de software en los sistemas operativos.	ISO 17799 10.4.1
Existen y se cumplen procedimientos de control de cambios para las actualizaciones y modificaciones previstas del software.	ISO 17799 10.4.1
Existen y se cumplen procedimientos de control de cambios para las modificaciones de emergencia del software.	ISO 17799 10.4.1
Se protegen y controlan las pruebas sobre los datos.	ISO 17799 10.4.2
Se mantienen estrictos controles de acceso sobre los códigos fuente de librerías y programas.	ISO 17799 10.4.3
La implementación de cambios se encuentra estrictamente controlada mediante el uso de procedimientos formales de control de cambios, con el fin de minimizar el riesgo de la adulteración de los sistemas informáticos.	ISO 17799 10.5.1 RFC 2527 4.6.6.1 X9.79 A
Controles de acceso de red	
Los sistemas de aplicación son revisados y probados cuando se producen cambios en los sistemas operativos.	ISO 17799 10.5.2
Se evitan las modificaciones innecesarias a los paquetes de software y los cambios esenciales son estrictamente controlados.	ISO 17799 10.5.3
La compra, el uso y la modificación del software son controlados y verificados para protegerse contra posibles ataques sorpresivos y códigos troyanos.	ISO 17799 10.5.4
Se aplican controles adecuados para asegurar el desarrollo externo de software.	ISO 17799 10.5.5

ix. Administración de la continuidad de los servicios de certificación

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 22 de 66

Objetivos de control. ANF AC tiene que mantener controles que aseguren razonablemente:

- a) La continuidad de las operaciones en caso de desastre;
- b) La continuidad de las operaciones en caso de la vulneración de su clave privada, y
- c) Que se minimizan de potenciales interrupciones en el servicio a los suscriptores y usuarios, como resultado del cese de sus operaciones.

Procedimientos de control	Referencias
Proceso de administración de la continuidad de los servicios de certificación	
La Entidad de Certificación posee un proceso controlado de desarrollo y mantenimiento de sus planes de continuidad de los servicios de certificación.	ISO 17799 11.1.11
ANF AC posee una estrategia de planificación de la continuidad de los servicios de certificación basada en una adecuada evaluación de riesgos.	ISO 17799 11.1.2
ANF AC posee planes de continuidad de los servicios de certificación para mantener o restaurar sus operaciones en un plazo adecuado luego de la interrupción o falla de los procesos críticos del sistema.	ISO 17799 11.1.3
ANF AC tiene un esquema de planificación de la continuidad de su sistema que requiere que los planes correspondientes incluyan: <ul style="list-style-type: none"> a) Las condiciones para activar los planes. b) Los procedimientos de emergencia. c) Los procedimientos de resguardo. d) Los procedimientos de reinicio de actividades. e) El cronograma de mantenimiento. f) Los requisitos de confiabilidad y capacitación, y g) Las responsabilidades del personal involucrado. 	ISO 17799 11.1.4
Los planes de continuidad de los sistemas son probados regularmente para asegurar su actualización y efectividad.	ISO 17799 11.1.5
Los planes de continuidad de los sistemas son revisados y actualizados periódicamente para asegurar su continua efectividad.	ISO 17799 11.1.5
Los planes de continuidad de los sistemas definen un sistema aceptable de tiempos de interrupción del servicio, de recuperación y de promedio entre fallas.	
Los planes de continuidad de los sistemas incluyen procesos de recuperación ante desastres para todos los componentes críticos del sistema de ANF AC, incluyendo el hardware, el software y las claves, en caso de fallas en uno o más de sus componentes.	ISO 15782-1 7.5
Los planes de continuidad de los sistemas comprenden los procedimientos de recuperación utilizados si los recursos de hardware, software y/o datos resultan afectados y se encuentran bajo sospecha de estarlo.	RFC 2527 4.4.8.1 X9.79 A

Los planes de continuidad de los sistemas incluyen procedimientos para asegurar los servicios durante el período de tiempo posterior a un desastre natural o de otro tipo, y antes de restablecer un entorno seguro, ya sea en las instalaciones de ANF AC o en el sitio alternativo de procesamiento.	RFC 2527 4.4.8.4 X9.79 A
Se efectúan regularmente copias de resguardo de la información esencial del sistema y del software. Los requerimientos de seguridad de esas copias son consistentes con la naturaleza y los controles sobre la información resguardada.	ISO 17799 8.4.1
El equipamiento de emergencia y los medios y soportes de resguardo se encuentran situados a una distancia segura del sitio principal para evitar los daños causados por el desastre.	ISO 17799 7.1.3 RFC 2527 4.5.1.8 X9.79 A
Vulneración de clave	
El plan de continuidad de los servicios de certificación de ANF AC contempla como una situación de emergencia la vulneración o la sospecha de vulneración de su clave privada.	ISO 15782-1 7.5
En caso de vulneración o de sospecha de vulneración de la clave privada de ANF AC, los procedimientos de recuperación prevén la revocación y remisión de todos los certificados que fueron firmados con dicha clave privada.	ISO 15782-1 7.5 y J.1, X9.57 G.1
Los procedimientos de revocación utilizados en caso de compromiso de la clave privada de ANF AC y de revocación de su clave pública incluyen: a) Como restablecer un entorno seguro. b) Como revocar la clave pública vulnerada de la CA. c) Cómo distribuir la nueva clave pública entre los usuarios y d) Cómo re-emitir los certificados a los suscriptores.	RFC 2527 4.4.8.2 y 4.4.8.3 X9.79 A
En caso que ANF AC deba reemplazar su clave privada raíz, se establecen procedimientos para una revocación segura y autenticada de: a) La clave privada raíz a reemplazar. b) El conjunto de certificados emitidos por la CA firmados con la clave privada vulnerada. c) Las claves privadas de toda CA subordinada y sus correspondientes certificados	ISO 15782-1 7.5 X9.57 G.1 ISO15782-1 J1
El plan de continuidad de los servicios de certificación de ANF AC incluye provisiones respecto a las acciones a: a) Desarrollar ante la vulneración de la clave privada, quien debe ser notificado; b) Procedimientos a desarrollar sobre el software y el hardware del sistema; c) Claves simétricas y asimétricas; d) Certificados digitales ya emitidos; e) Datos cifrados.	
Cesación de actividades de la CA	

ANF AC mantiene procedimientos para la cesación de actividades, la notificación a terceros afectados y la transferencia de archivos relevantes a otra Entidad que estará a cargo de su custodia.	RFC 2527 4.4.9 X9.79 A
--	------------------------------

x. Comprobación y conformidad

Objetivos de control. ANF AC tiene que mantener controles que provean razonable seguridad de que:

- a) Cumple con todos los requerimientos legales establecidos para la Infraestructura de Clave Pública en los países en los que desarrolla su actividad;
- b) Se asegura el cumplimiento de las políticas y procedimientos de seguridad;
- c) Se maximiza la efectividad del proceso de auditoría y se minimizan las interferencias del/al mismo; y,
- d) Se detecta el uso no autorizado de los sistemas de la EPSC.

Procedimientos de control	Referencias
Conformidad con requerimientos legales	
ANF AC posee procedimientos que aseguran el cumplimiento de todos los requerimientos legales, de reglamentación y contractuales relevantes, los cuales se encuentran explícitamente definidos y documentados para cada sistema informático.	ISO 17799 12.1.1
Esta EPSC implementa procedimientos que aseguran el respecto de los derechos de la propiedad intelectual, y las condiciones de uso de productos de software adquirido bajo licencia.	ISO 17799 12.1.2
Se protegen de pérdida, destrucción y falsificación, los registros importantes de la organización.	ISO 17799 12.1.3
Existen procedimientos que aseguran que la información personal es protegida de acuerdo con las normas aplicables.	ISO 17799 12.1.4
La gerencia autoriza el uso de servicios de procesamiento y se establecen controles para prevenir el uso indebido de los mismos.	ISO 17799 12.1.5
Se establecen controles que aseguren cumplimiento de acuerdos nacionales, leyes, regulaciones y otros instrumentos a fin de controlar el acceso o utilización de software y hardware criptográfico.	ISO 17799 12.1.6

<p>Las políticas y procedimientos de seguridad deben incluir el tratamiento de los siguientes temas:</p> <ul style="list-style-type: none"> a) Las clases de información que ANF AC y las Autoridades de Registro deben mantener confidencial. b) Las clases de información que no es considerada confidencial, c) Quien está autorizado a ser informado de las razones de la revocación y suspensión de certificados. d) La política de difusión de información ante requerimientos judiciales. e) La información que puede ser revelada como parte de una acción civil. f) Las condiciones bajo las cuales ANF AC o las AR's pueden revelar información ante el requerimiento del titular de dicha información. g) Toda otra circunstancia en la cual puede difundirse información confidencial. 	RFC 2527 4.2.8 X9.79 A
Revisión de la política de seguridad y conformidad técnica	
La gerencia es responsable de asegurar que los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente.	ISO 17799 12.2.1
Las operaciones de ANF AC están sujetas a revisiones regulares para asegurar el cumplimiento de las políticas y estándares de seguridad.	ISO 17799 12.2.1
Los sistemas de ANF AC son controlados periódicamente para verificar el cumplimiento de los estándares de implementación de seguridad.	ISO 17799 12.2.2
Consideraciones sobre auditoria de sistemas.	
La auditoria de los sistemas en operación es planificada y acordada de manera de minimizar los riesgos de interrupciones en los procesos del negocio.	ISO 17799 12.3.1
El acceso a las herramientas de auditoria de sistemas es protegido para prevenir compromisos o posibles usos indebidos.	ISO 17799 12.3.2
Acceso y uso del sistema de comprobación	
Se establecen procedimientos de monitorización del uso de los sistemas de ANF AC y se revisan periódicamente los resultados de dichas comprobaciones.	ISO 17799 9.7.2

xi. Registro de eventos

Objetivos de control. ANF AC tiene que mantener controles que provean un nivel razonable de seguridad de que:

- a) Los eventos significativos referidos al ambiente de la CA;

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 26 de 66

- b) La administración de claves y de certificados son registrados en forma adecuada y completa;
- c) Se mantiene la confidencialidad e integridad de los registros de eventos actuales y archivados;
- d) Los registros de eventos se archivan en forma completa y confidencial de acuerdo con las prácticas del negocio, y,
- e) Los registros de eventos son revisados periódicamente por personal autorizado.

Procedimientos de control	Referencias
Registro de eventos	
ANF AC genera registros de eventos en forma electrónica y manual según sea más apropiado.	X9.57 6 ISO 15782-1 7.4.1
<p>Todos los registros incluyen los siguientes elementos:</p> <ul style="list-style-type: none"> a) Fecha y hora del registro. b) Número de serie o secuencia del registro. c) Tipo de registros. d) Fuente del registro (ej.: terminal, puerto, etc.) e) Identificación de la entidad que efectuó el registro. 	ISO 15782-1 F.1.1 X 9.57 D.1.1 RFC 2527 4.4.6.5 X9.79 A
Eventos registrados	
<p>ANF AC registra los siguientes eventos relativos a la administración del ciclo de vida de las claves:</p> <ul style="list-style-type: none"> a) Generación del par de claves de ANF AC (y del suscriptor, de ser aplicable) b) Instalación de claves criptográficas manuales y sus resultados (con identidad del operador). c) Resguardo de las claves de ANF AC. (*2) d) Almacenamiento de las claves de ANF AC. e) Recuperación de las claves de ANF AC. f) Actividades de custodia de las claves (key escrow) de la CA. g) Utilización de las claves de ANF AC. h) Archivo de las claves de ANF AC. i) Retiro de servicio de datos relacionados con las claves. j) Destrucción de claves de ANF AC. k) Identificación de la entidad que autoriza una operación de administración de claves. l) Identificación de la entidad que maneja datos relativos a las claves (tal como componentes de claves, o claves almacenadas en dispositivos portátiles u otros medios). m) Custodia de las claves o de dispositivos o medios que almacenan las claves. n) Vulneración de la clave privada. 	

<p>ANF AC registra los siguientes eventos relativos a la administración del ciclo de vida del certificado:</p> <ul style="list-style-type: none"> a) Recepción de requerimientos de certificados –incluyendo requerimiento inicial, solicitud de renovación y de remisión de claves–. b) Transferencia de claves públicas para su certificación. c) Cambios en los datos de identificación de una entidad. d) Generación de certificados. e) Distribución de la clave pública de ANF AC. f) Solicitudes de revocación de certificados. g) Solicitudes de suspensión de certificados. h) Generación y emisión de certificados revocados, y i) Acciones tomadas relativas a la expiración de un certificado. 	<p>ISO 15782-1 F.1.6 X 9.57 D.1.6 RFC 2527 4.4.5.1 y 4.4.6.1 X9.79 A</p>
<p>ANF AC registra los siguientes eventos relativos a la administración del ciclo de vida de los dispositivos criptográficos:</p> <ul style="list-style-type: none"> a) Recepción del dispositivo. b) Ingreso o retiro del dispositivo del lugar de almacenamiento. c) Utilización de dispositivos. d) Desinstalación del dispositivo. e) Remisión de un dispositivo para servicio técnico o reparación. f) Retiro/Baja / Descarga de un dispositivo. 	<p>ISO 10202-1 4d</p>
<p>ANF AC registra (o requiere que las AR's registren) la siguiente información sobre los requerimientos de certificados:</p> <ul style="list-style-type: none"> a) Tipo/s de documento/s identificatorio/s presentado/s por el solicitante. b) Registro de datos o números de identificación unívocos. c) Localización del archivo de las copias de las solicitudes de certificados y de los documentos de identificación. d) Identificación de la entidad que acepta la solicitud. e) Método utilizado para validar los documentos de identificación, y f) Nombre de los operadores que intervienen en el proceso. 	<p>ISO 16782-1 F.1.2 X9.57 D.1.2</p>
<p>ANF AC registra los siguientes eventos de seguridad:</p> <ul style="list-style-type: none"> a) Archivos de seguridad sensibles o registros leídos o escritos, incluyendo el registro diario de eventos. b) Borrado de datos de seguridad sensibles. c) Cambios en los perfiles de seguridad. d) Utilización de mecanismos de identificación y autenticación, hayan o no sido autorizados (incluyendo intentos múltiples de autenticación fallida). e) Caídas del sistema, fallas en el hardware y otras anomalías. f) Acciones desarrolladas por los operadores y administradores del sistema y/u oficiales de seguridad informática. g) Cambios de/ en los datos identificación. h) Decisiones de obviar procesos de encriptación/autenticación y i) Accesos al sistema de ANF AC o a cualquier componente relacionado. 	<p>ISO 16782-1 F.1.5 X9.57 D.1.5</p>
<p>Los registros de eventos no reflejan los valores en texto plano de ninguna clave privada.</p>	<p>X 9.57 6 ISO15782-1 7.4.1</p>

Los sistemas de horario de los servidores están sincronizados para permitir un adecuado registro de eventos.	ISO 17799 9.7.3
Protección de registro de eventos	
Los registros de eventos actuales y archivados se mantienen de manera tal de prevenir modificaciones o destrucciones no autorizadas.	X9.57 6 ISO15782-1 7.4.1 RFC 2527 4.4.5.4 y 4.4.6.3 X9.79 A
Los registros de eventos automatizados en proceso y los archivados, se encuentran protegidos contra modificaciones o alteraciones.	X9.57 6 ISO15782-1 7.4.1 RFC 2527 4.4.5.4 y 4.4.6.3 X9.79 A
La clave privada utilizada para firmar los registros de eventos no es utilizada para ningún otro propósito.	X9.57 6 ISO 15782-1 7.4.1
Archivo de registro de eventos	
Los registros de eventos de ANF AC son archivados con una periodicidad predeterminada.	ISO15782-1 F.2 X9.57 D.2 RFC 2527 4.4.5.5 X9.79 A
Se ha efectuado una evaluación de riesgos para determinar el tiempo adecuado de conservación de los registros de eventos, teniendo en cuenta las normas aplicables.	RFC 2527 4.4.5.3 y 4.4.6.2 X9.79 A
ANF AC mantiene el archivo de los registros de eventos en un sitio seguro fuera de sus instalaciones y por un período preestablecido.	ISO15782-1 F.2 RFC 2527 4.4.5.3, 4.4.5.5, 4.4.6.2 y 4.4.6.4 X9.79 A
Revisión de registro de eventos	
Los registros de eventos actuales y archivados sólo pueden ser revisados por personal autorizado y por razones justificadas relativas a la operación del negocio o a la seguridad.	ISO15782-1 7.4.1 RFC 2527 4.4.5.4 y 4.4.6.3 X9.79 A
Los registros de eventos son revisados periódicamente.	X9.57 6 ISO 15782-1 7.4.2 RFC 2527 4.4.5.2 X9.79 A
La revisión de los registros de eventos actuales y archivados incluye una validación de su integridad, y la identificación y seguimiento de actividades excepcionales, no autorizadas o sospechosas.	X9.57 6 ISO 15782-1 7.4.2 RFC 2527 4.4.6.7 X9.79 A

(*2)

El estándar ANS 9.79:2001 considera en la extensión de lo citado a las claves del suscriptor. Debido a que el marco legal y la propia CPS y CP's no permiten a ANF AC mantener copia de la clave privada del suscriptor, ni tan siquiera se ofrece el servicio de generación del par de claves, es por lo que se elimina esa posibilidad en este documento.

xii. Seguridad Criptográfica

Objetivos de control. ANF AC tiene que utilizar algoritmos criptográficos y parámetros (longitud de clave) considerados seguros.

Procedimientos de control	Referencias
Algoritmos Seguros	
ANF AC sólo debe de utilizar algoritmos y parámetros de algoritmo calificados como seguros, en todos los dispositivos seguros de creación de firma.	CWA-14167-2 3.4 P.Algorithms

IV.b Controles sobre la administración del ciclo de vida de las claves

i. Generación de las claves de ANF AC

Objetivos de control. ANF AC tiene que mantener controles que aseguran razonablemente que su par de claves se generan de acuerdo con estándares reconocidos (*3) adoptados por la Infraestructura de Claves Públicas (PKI) de los países en los que opera.

Procedimientos de control	Referencias
Generación de claves de ANF AC	
La generación de claves de ANF AC se realiza de acuerdo a lo dispuesto por las normas y estándares aplicables en la normativa europea y otros estándares internacionales, sobre la base de una evaluación de riesgos y a los requerimientos del sistema y de acuerdo a las prácticas de certificación publicadas por ANFAC.4	ISO 15782-1 7.3.1.1 FIPS 140-1 X9.79
La generación de claves de ANF AC requiere un control estricto por parte del personal debidamente autorizado.	X9.57 4.2.4
ANF AC genera su propio par de claves en el mismo dispositivo criptográfico en el cual dicho par será utilizado, o bien el par de claves es introducido directamente desde el dispositivo en que fue generado al dispositivo en que será utilizado, dependiendo del caso y si fuera aplicable.	ISO 11568-5 5.1.2
La generación de claves utiliza un número generador aleatorio (RSN) o bien un pseudo número generador aleatorio (PRNG), según se especifica en los estándares aplicables.	X9.80 ISO 11568-5 5.1.2

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 30 de 66

La generación de claves utiliza un número generador primo según se especifica en los Estándares Tecnológicos reseñados en la CPS de ANF AC y según los estándares internacionales en la materia.	X9.82
La generación de claves utiliza un algoritmo de generación según lo especificado en los Estándares Tecnológicos reseñados en la CPS de ANF AC y según los estándares internacionales en la materia.	X9.30 X9.31 X9.62 CWA-14167-2 3.4 P.Algorithms
La generación permite obtener una longitud de claves acorde a lo dispuesto en la CPS de ANF AC y según los estándares internacionales en la materia.	X9.30 X9.31 X9.62 RFC 2527 4.6.1.5 X9.79 A
La integridad del hardware/software utilizado para la generación de claves, así como las interfaces hacia el hardware/software, son probadas antes de su utilización.	ISO 15782-1 7.3.1.1

(*3)

El estándar X9.79, en estos casos señala estándares que son reconocidos internacionalmente.

ii. Almacenamiento, back up y recuperación de claves de ANF AC

Objetivos de control. ANF AC tiene que mantener controles que otorguen un nivel razonable de seguridad de que las claves privadas permanecen confidenciales y que se mantiene su integridad.

Procedimientos de control	Referencias
Almacenamiento, backup y recuperación de claves de ANF	
La clave privada de firma de ANF AC se almacena de conformidad con las exigencias de nivel apropiado establecidas por los Estándares Tecnológicos internacionales, en base a una evaluación de riesgos y a los requerimientos del sistema PKI y de acuerdo a la CPS y CP's	ISO 15782-1 FIPS 140-1/ X9.66
La clave privada de firma de ANF AC es transferida desde un módulo criptográfico seguro para garantizar el almacenamiento, que permita efectuar el procesamiento off line o back up y recuperación, será exportada en un esquema de administración segura de claves incluyendo alguno de los siguientes: a) Como texto cifrado utilizando una clave debidamente segura. b) Como fragmentos cifrados de clave utilizando un doble control y conocimiento compartido. c) En otro módulo criptográfico seguro tal como un dispositivo de transporte de clave utilizando un doble control.	ISO 15782 7.3.1.2

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 31 de 66

Si se efectúa una copia de resguardo de la clave privada de firma de ANF AC la misma es copiada, almacenada y recuperada por personal autorizado utilizando un doble control en un entorno físicamente seguro.	ISO 15782 7.3.1.1
Si se efectúan copias de resguardo de la clave privada de firma de ANF AC, las mismas se encuentran sujetas a similares o a mayores controles de seguridad que las claves en uso.	ISO 11568-5 4.5.5 ISO 15782-1 7.3.1.2
Si se efectúan copias de resguardo de la clave privada de firma de ANF AC, la recuperación de la misma se efectúa en el mismo entorno seguro utilizado en el proceso de back up, utilizando un doble control.	ISO 15782-1 7.3.1.1

iii. Distribución de la clave pública de ANF AC

Objetivos de control. ANF AC tiene que mantener controles que provean un nivel razonable de seguridad acerca del mantenimiento de la integridad y autenticidad de su clave privada y de cualquier parámetro asociado, durante la distribución inicial y subsiguiente.

Procedimientos de control	Referencias
Distribución de la clave pública de ANF AC	
ANF AC provee un mecanismo para detectar modificaciones de su clave pública durante el proceso inicial de distribución (por ejemplo: utilizando un certificado autofirmado).	ISO 15782-1 7.3.5 X9.57 4.2.3 ISO 11568-5 4.7
El mecanismo inicial de distribución para la clave pública de ANF AC es controlado según lo especificado en su CPS y CP's	X9.57 4.2.3
Las claves públicas de ANF AC son distribuidas inicialmente utilizando uno de los siguientes métodos, de acuerdo a lo establecido en su CPS: a) Medios legibles por el equipo (ej.: smartcard). b) Contenido en un módulo criptográfico. c) Otro medio considerado seguro.	ISO 15782-1 7.3.5
El subsiguiente mecanismo de distribución para la clave pública de la ANF AC es controlado y documentado en la CPS de la EPSC.	X9.57 4.2.3

<p>Si una entidad ya posee una copia autenticada de la clave pública de ANF AC, se distribuirá una nueva clave pública utilizando uno de los siguientes métodos de acuerdo a lo establecido en la CPS de ANF AC:</p> <ul style="list-style-type: none"> a) Transmisión electrónica directa desde ANF AC. b) Ubicándola en un directorio o “cache” remoto. c) Cargándola en un módulo criptográfico. d) Cualquiera de los métodos utilizados para la distribución inicial. 	<p>ISO 15782-1 7.3.5</p>
---	------------------------------

iv. Custodia de las claves de ANF AC

Objetivos de control. ANF AC tiene que mantener controles que garanticen razonablemente la confidencialidad de sus claves privadas, en el caso en que las entregue en custodia.

Procedimientos de control	Referencias
Custodia de las claves de ANF AC	
<p>Si una tercera parte provee servicios de custodia, existe un contrato firmado por las partes estableciendo responsabilidades y recursos legales, y la exigencia de que dicha parte no tenga acceso a las claves y a sus datos de activación.</p>	
<p>Si las claves privadas se encuentran en custodia, las copias custodiadas de la clave privada de firma de ANF AC se encuentran sujetas a similares o mayores niveles de controles de seguridad que las claves en uso.</p>	<p>ISO 11568-5 4.5.5</p>

v. Utilización de las claves de ANF AC

Objetivos de control. ANF AC tiene que mantener controles que aseguren razonablemente que sus claves son utilizadas únicamente para las funciones previstas, y en sus ubicaciones predeterminadas.

Procedimientos de control	Referencias
Utilización de las claves de ANF AC	
<p>La activación de la clave privada de firma de ANF AC se realiza utilizando controles multipartes.</p>	
<p>De ser necesario, basado en una evaluación de riesgos, la activación de la clave privada de ANF AC se realiza utilizando autenticación de factores múltiples (por ejemplo: smartcard y password, biometría y password).</p>	<p>ISO 11568-5 4.5.5</p>

ANF AC deja de utilizar su par de claves al final del período de vigencia o bien cuando se conoce o sospecha de la vulneración de su clave privada.	ISO 11568-5 4.9
---	--------------------

vi. Destrucción de las claves de ANF AC

Objetivos de control. ANF AC tiene que mantener controles que aseguren razonablemente que sus claves se destruyen por completo al finalizar su ciclo de vida.

Procedimientos de control	Referencias
Destrucción de las claves de ANF AC	
La autorización de destrucción de una clave privada de ANF AC y el procedimiento a seguir (por ejemplo: destrucción del token, reescritura de la clave) se encuentran delimitados, según lo previsto en su CPS.	RFC 2527 4.6.2.9 X9.79 A
Todas las copias y fragmentos de la clave privada de la Entidad de Certificación se destruyen al finalizar el ciclo de vida de su par de claves.	
Si un dispositivo criptográfico seguro es accesible, y se encuentra permanentemente fuera del servicio, todas las claves privadas de la ANF AC almacenadas dentro del dispositivo que hayan sido utilizadas o potencialmente puedan ser usadas con propósitos criptográficos, son destruidas.	ISO 11568-5 4.13
Si un dispositivo criptográfico seguro está siendo apartado permanentemente del servicio, todas las claves contenidas dentro del dispositivo que hayan sido usadas con propósitos criptográficos, son borradas del mismo.	ISO 13491-1 A.2.6.A49
Si el contenedor de un dispositivo criptográfico tiene por finalidad proveer evidencia de falsificaciones y el dispositivo se encuentra permanentemente fuera del servicio, dicho contenedor deber ser también destruido.	ISO 13491-1 A.2.6.A50

vii. Archivo de las claves de ANF AC

Objetivos de control. ANF AC tiene que mantener controles que permitan proveer un nivel razonable de seguridad de que las claves archivadas permanecen confidenciales y nunca son reutilizadas.

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 34 de 66

Procedimientos de control	Referencias
Archivo de las claves de ANF AC	
Las claves de ANF AC que se encuentran archivadas están sujetas a similares o mayores controles de seguridad que aquellas que se encuentran en uso.	ISO 11568-5 4.5.5 X9.24 3.8
Todas las claves de ANF AC que se encuentran archivadas se destruyen al finalizar su período de archivo, utilizando un doble control en un sitio físicamente seguro.	
Las claves archivadas nunca son reutilizadas.	
Las claves archivadas son recuperadas por el tiempo mínimo técnicamente permitido.	
Las claves archivadas son verificadas periódicamente para asegurar que son debidamente destruidas al final de su período de archivo.	

viii. Administración del ciclo de vida del hardware criptográfico

Objetivos de control. ANF AC tiene que mantener controles que aseguran razonablemente que:

- a) El acceso al hardware criptográfico de ANF AC se limita al personal autorizado,
- b) El hardware criptográfico funciona adecuadamente.

A los fines de este capítulo, "hardware criptográfico" de la Entidad de Certificación se refiere a dispositivos que contienen las claves privadas de firma de ANF AC.

Procedimientos de control	Referencias
Manejo de dispositivos	
Las políticas y procedimientos requieren que el hardware criptográfico de ANF AC sea enviado por el proveedor por correo certificado o por cualquier otro medio, utilizando embalaje inviolable.	ISO 13491-1 A.2.4.A40
A la recepción del envío del hardware criptográfico efectuado por el proveedor por parte de personal autorizado de ANF AC, dicho personal efectuará una revisión del embalaje para determinar si se encuentra intacto.	ISO 13491-1 A.2.4.A40

<p>Para prevenir fraudes, el hardware criptográfico de ANF AC es almacenado en un sitio seguro, cuyo acceso está limitado a personal autorizado, con las siguientes características:</p> <ul style="list-style-type: none"> a) Procesos de control de inventarios y procedimientos para administrar el origen, recepción, condiciones, salida y destino de cada dispositivo. b) Procesos de control de acceso y procedimientos para limitar el acceso físico a personal autorizado. c) Todos los intentos de acceso, autorizados o no, a los servicios de la EPSC y al mecanismo de almacenamiento de los dispositivos ingresados en un registro de eventos. d) Procesos de incidentes y procedimientos para manejar eventos anormales, brechas de seguridad, investigaciones y reportes. e) Procesos de auditoría y procedimientos para verificar la efectividad de los controles. 	<p>ISO 13491-1 A.2.4.A42</p>
<p>El hardware criptográfico de ANF AC es almacenado en embalajes inviolables.</p>	<p>ISO 13491-1 E.E2.E12</p>
<p>El manejo del hardware criptográfico de ANF AC se efectúa en presencia de no menos de dos empleados confiables.</p>	<p>X9.57 4.2.4 ISO15782-1 7.3.1.1 ISO 13491-1 E.E2.E12</p>
<p>La instalación del hardware criptográfico de ANF AC se efectúa en presencia de no menos de dos empleados confiables.</p>	<p>ISO15782-1 7.3.1.1 ISO 13491-1 E.E2.E12</p>
<p>La eliminación del hardware criptográfico de ANF AC de producción se efectúa en presencia de no menos de dos empleados confiables.</p>	<p>X9.57 4.2.4 ISO15782-1 7.3.1.1 ISO 13491-1 E.E2.E12</p>
<p>El proceso de reparación o servicio del hardware criptográfico, utilizando nuevo hardware, software o soportes lógicos, se efectúa en presencia de no menos de dos empleados confiables.</p>	<p>X9.57 4.2.4 ISO15782-1 7.3.1.1 ISO 13491-1 E.E2.E12</p>
<p>El lugar de prestación del servicio de mantenimiento, soporte técnico o reparaciones es un sitio seguro con control de inventario y acceso limitado a personal autorizado.</p>	
<p>El proceso por el cual el hardware criptográfico de ANF AC es desmantelado y retirado del uso se efectúa en presencia de por lo menos dos empleados confiables.</p>	<p>X9.57 4.2.4 ISO15782-1 7.3.1.1 ISO 13491-1 E.E2.E12</p>

Utilización de dispositivos	
Se efectúa un test de aceptación y verificación de los soportes lógicos al momento de la recepción del hardware de ANF AC proveniente del fabricante.	ISO 13491-1 A.2.3.A38
Contra la recepción del hardware de ANF AC que haya sido reparado, se efectúa un test de aceptación y verificación de los soportes lógicos.	ISO 13491-1 A.2.3.A38
Se efectúa un test de aceptación y verificación de los soportes lógicos al momento de la recepción del hardware de ANF AC proveniente del fabricante.	ISO 13491-1 A.2.3.A38
Los dispositivos utilizados para almacenamiento y recuperación de la clave privada y sus interfaces son sometidos a un test de integridad antes de su utilización.	
Se verifica periódicamente el correcto procesamiento del hardware criptográfico de ANF AC.	ISO 13491-1 A.2.3.A43
Se efectúa un diagnóstico durante el test de verificación de problemas del hardware criptográfico de ANF AC, en presencia de no menos de dos empleados confiables.	

IV.c Controles sobre el ciclo de vida del certificado

i. Registro del suscriptor

Objetivos de control. ANF AC tiene que mantener controles que provean razonable seguridad con relación a que:

- Los suscriptores sean debidamente identificados y autenticados, y
- Las solicitudes de certificados sean adecuadas, autorizadas y completas.

Procedimientos de control	Referencias
<i>Nota:</i> una "entidad solicitante" puede ser un suscriptor que solicite un certificado a ANF AC o a una AR, una AR que solicite un certificado de ANF AC.	
Identificación y autenticación	
ANF AC verifica o requiere que la AR externa verifique la identidad de la entidad solicitante de un certificado de acuerdo a lo dispuesto por la CPS de ANF AC y la CP aplicable.	ISO 15782-1 7.3.3 X9.57 4.2.1 X9.57 4.4.2

ANF AC requiere que la entidad solicitante deba preparar y remitir los datos requeridos en la solicitud del certificado a la AR (o a ANF AC) según se especifica en la CPS y CP de ANF AC.	ISO 15782-1 7.3.2 X9.57 4.4.1
ANF AC verifica o requiere que la AR externa verifique la autoridad de la entidad solicitante de acuerdo con la CPS y la CP aplicable al certificado que solicita.	RFC 2527 4.3.1.8 y 4.3.1.9 X9.79 A
ANF AC verifica o requiere que la AR externa verifique la veracidad de la información incluida en el requerimiento del certificado de la entidad solicitante de acuerdo a lo establecido en la CPS y la CP aplicable.	
Si se utilizan ARs externas, ANF AC valida la identidad de las mismas.	
Si se utilizan ARs externas, ANF AC las autoriza de acuerdo a lo establecido en su CPS y CP's.	
Requerimiento de certificado	
ANF AC requiere que la entidad solicitante prepare y envíe los datos apropiados del requerimiento a ANF AC o a una AR externa, según se especifica en la CPS o CP's aplicables en cada caso.	ISO 15782-1 7.3.2 X9.57 4.4.1
ANF AC requiere que la entidad solicitante remita su clave pública en un mensaje firmado a ANF AC para la emisión del certificado correspondiente. La Entidad de Certificación requiere que la entidad solicitante firme digitalmente el requerimiento utilizando la clave privada que se vincula con la clave pública contenida en el requerimiento de manera tal que: a) Permita la detección de errores en el proceso de solicitudes, b) Pruebe la posesión de la clave privada para la clave pública registrada.	ISO 15782-1 7.3.2 X9.57 4.4.1 RFC 2527 4.3.1.7 X9.79 A
ANF AC utiliza la clave pública contenida en el requerimiento de certificado de la entidad solicitante para verificar la firma de ésta en el requerimiento remitido.	ISO 15782-1 7.3.3 X9.57 4.4.4
Si se utiliza una AR externa, ANF AC requiere que la misma remita el requerimiento del certificado de la entidad solicitante a ANF AC en un mensaje (requerimiento) firmado por la AR.	X9.57 4.7.1.d
Si se utiliza una AR externa, ANF AC requiere que la AR asiente sus actividades en un registro de eventos.	X9.57 4.4.4 y 4.7.1.j
Si se utiliza una AR externa, ANF AC verifica la autenticidad de la solicitud remitida por la AR de acuerdo con la CPS y CP aplicable en cada supuesto.	ISO 15782-1 7.3.4

Si se utiliza una AR externa, ANF AC verifica la firmade la AR en el requerimiento de certificado.	ISO 15782-1 7.3.4
ANF AC o la AR verifica la solicitud del certificado para evitar errores u omisiones de acuerdo a lo establecido en la CPS y CP's de ANF AC.	ISO 15782-1 7.3.3
ANF AC verifica la unicidad del nombre distintivo de la entidad solicitante dentro del dominio de ANF AC.	ISO 15782-1 7.3.4 ISO 9594/X.509 11.2 X9.57 4.4.4
ANF AC acepta los requerimientos de certificados de la entidad solicitante cuya identidad haya sido validada.	ISO 15782-1 7.3.3 X.57 4.4.3
Cuando ANF AC detecta claves públicas duplicadas, el requerimiento de certificado es rechazado y el certificado original es revocado.	ISO 15782-1 7.3.4.4

ii. Renovación de certificados

Objetivos de control. ANF AC tiene que mantener controles que aseguren razonablemente que las solicitudes de renovación de certificados son adecuadas, autorizadas y completas.

Procedimientos de control	Referencias
Requerimiento de renovación de certificados	
El requerimiento de renovación del certificado del suscriptor incluye al menos su nombre distintivo, su número de serie (u otra información que lo identifique), y el período de validez solicitado para permitir a ANF AC o a la AR identificar el certificado a renovar.	ISO 15782-1 7.3.9
ANF AC requiere que la entidad solicitante firme digitalmente la solicitud de renovación de certificado utilizando la clave privada que se vincula con la clave pública contenida en el certificado vigente de la entidad solicitante.	ISO 15782-1 7.3.9
ANF AC o la AR procesan los datos de renovación del certificado para verificar la identidad de la entidad solicitante e identificar el certificado a renovar.	ISO 15782-1 7.3.9
ANF AC o la AR validan la firma en el requerimiento de renovación del certificado.	ISO 15782-1 7.3.9
ANF AC o la AR verifican la existencia y validez del certificado a renovar.	ISO 15782-1 7.3.9

ANF AC o la AR verifican que el requerimiento, incluida la extensión del período de validez, cumple los requerimientos establecidos en las practicas de certificación de ANF AC.	ISO 15782-1 7.3.9
Si se utiliza una AR externa, ANF AC requiere que de la AR externa que remita a ANF AC los datos del requerimiento de certificado de la entidad solicitante, en un mensaje (requerimiento de renovación) firmado por la AR.	X9.57 4.7.1.d
Si se utiliza una AR externa, ANF AC requiere que la AR cumpla en forma segura la parte del proceso de renovación sobre el cual posee responsabilidad.	X9.57 4.7.1.i
Si se utiliza una AR externa, ANF AC requiere que la AR asiente sus actividades en un registro de eventos.	X9.57 4.7.1.j
Si se utiliza una AR externa, ANF AC verifica la autenticidad de la solicitud remitida por la AR, de acuerdo a lo dispuesto en la CPS y CP's de ANF AC.	ISO 15782-1 7.3.4
Si se utiliza una AR externa, ANF AC verifica la firma de la AR en el requerimiento de certificado.	ISO 15782-1 7.3.4
ANF AC o la AR verifican el requerimiento de renovación del certificado para evitar errores u omisiones.	ISO 15782-1 7.3.3
ANF AC o la AR notifican a los suscriptores, previo a la expiración de su certificado, acerca de la necesidad de efectuar la renovación de acuerdo con lo establecido en las prácticas de certificación publicadas por ANF AC.	
Previo a la generación y emisión de certificados renovados, la ANF AC o la AR verifican: a) La firma en la solicitud de renovación. b) La existencia y validez del certificado a ser renovados, y c) Que el requerimiento, incluyendo la extensión del período de validez, cumple los requerimientos establecidos en las prácticas de certificación publicadas por ANF AC.	ISO 15782-1 7.3.9

iii. Re-emisión de las claves del certificado

Objetivos de control. ANF AC tiene que mantener controles que aseguren razonablemente que:

- a) Las solicitudes de re-emisión son adecuadas, autorizadas y completas y
- b) Las solicitudes de re-emisión posteriores a una revocación o expiración son adecuadas, autorizadas y completas.

Procedimientos de control	Referencias
---------------------------	-------------

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 40 de 66

Requerimientos rutinarios de re-emisión	
Los requerimientos de re-emisión de certificados del suscriptor incluyen al menos el nombre distintivo del suscriptor, el número de serie del certificado y el período de validez requerido para permitir que ANF AC o la AR identifiquen el certificado a re-emitir.	ISO 15782-1 7.3.9
ANF AC requiere que la entidad solicitante firme digitalmente el requerimiento de re-emisión del certificado utilizando la clave privada que se vincula con la clave pública contenida en el certificado vigente de la entidad solicitante.	ISO 15782-1 7.3.9
ANF AC o la AR procesan el requerimiento de re-emisión del certificado para verificar la identidad de la entidad solicitante e identificar el certificado a ser re-emitido.	ISO 15782-1 7.3.9
ANF AC o la AR validan la firma en el requerimiento de renovación del certificado.	ISO 15782-1 7.3.9
ANF AC o la AR validan la firma en el requerimiento de re-emisión del certificado.	ISO 15782-1 7.3.9
ANF AC o la AR verifican la existencia y validez del certificado a ser re-emitido.	ISO 15782-1 7.3.9
ANF AC o la AR verifican que el requerimiento de re-emisión del certificado cumple los requerimientos establecidos en las prácticas de certificación de ANF AC.	ISO 15782-1 7.3.9
Si se utiliza una AR externa, ANF AC requiere que dicha Unidad le envíe la solicitud de re-emisión del certificado de la entidad solicitante en un mensaje firmado por la AR.	X9.57 4.7.1.d
Si se utiliza una AR externa, ANF AC requiere que la AR cumpla en forma segura la parte del proceso de re-emisión sobre el cual posee responsabilidad.	X9.57 4.7.1.i
Si se utiliza una AR externa, ANF AC requiere que dichas Unidades asienten sus actividades en un registro de eventos.	X9.57 4.7.1.j
Si se utiliza una AR externa, ANF AC verifica la autenticidad de la solicitud remitida por la AR.	ISO1578 2-1 7.3.4
Si se utiliza una AR externa, ANF AC verifica la firma de la AR en el requerimiento de re-emisión del certificado.	ISO 15782-1 7.3.4
ANF AC o la AR verifican el requerimiento de re-emisión del certificado para evitar errores u omisiones.	ISO 15782-1 7.3.3
ANF AC o la AR notifican a sus suscriptores, previo a la expiración de sus certificados, acerca de la necesidad de re-emisión.	

<p>Previo a la generación y emisión de certificados reemitidos, la ANF AC o la AR verifican lo siguiente:</p> <ul style="list-style-type: none"> a) La firma en la solicitud de reemisión enviada. b) La existencia y validez del certificado a ser reemitido. c) Que los requerimientos cumplan lo dispuesto en las prácticas de certificación de ANF AC. 	<p>ISO 15782-1 7.3.9</p>
<p>Reemisión posterior a la revocación o expiración</p>	
<p>Producida la revocación o expiración del certificado vigente del suscriptor, éste deberá seguir los procedimientos de registro establecidos por ANF AC a fin de obtener un nuevo certificado (re-emitido) de acuerdo con lo establecido en las prácticas de certificación de ANF AC.</p>	<p>RFC 2527 4.3.3 X9.79 A</p>

iv. Re-emisión de las claves del certificado

Objetivos de control. ANF AC tiene que mantener controles que aseguren razonablemente que los certificados nuevos, renovados y re-emitidos sean generados y emitidos de acuerdo con sus políticas, prácticas y procedimientos establecidos.

Procedimientos de control	Referencias
<p>Emisión del certificado.</p>	
<p>ANF AC genera certificados utilizando el formato apropiado según lo establecido en la CPS y CP's en vigor.</p>	<p>RFC 2527 4.7.1 X9.79 A</p>
<p>ANF AC genera certificados de acuerdo a lo establecido en los Estándares Tecnológicos que se establecen en la CPS y CP's de ANF AC.</p>	<p>ISO 15782-1 8.5.5 ISO 9594/X.509 12.4.2</p>
<p>Los períodos de validez de los certificados se establecen de acuerdo a lo establecido en los Estándares Tecnológicos que se establecen en la CPS y CP's de ANF AC.</p>	<p>ISO 15782-1 8.5.5 ISO 9594/X.509 12.4.2</p>
<p>Las extensiones de los certificados se establecen de acuerdo a lo establecido en los Estándares Tecnológicos que se establecen en la CPS y CP's de ANF AC.</p>	<p>X9.55 ISO 15782-1 8.5.10 ISO 9594/X509 12.4.2</p>
<p>Las extensiones de utilización de clave se establecen de acuerdo a lo establecido en los Estándares Tecnológicos que se establecen en la CPS y CP's de ANF AC.</p>	<p>ISO 15782-1 9.1.3 ISO 9594/X.509 12.2.2.3</p>

ANF AC firma el certificado de la entidad solicitante con su clave privada de firma.	ISO 15782-1 4.4
ANF AC emite el certificado luego que el mismo ha sido aceptado por la entidad solicitante de acuerdo a lo establecido en la CPS y CP's de ANF AC.	
Cuando se utiliza una AR, ANF AC le notifica cuando se ha emitido un certificado a un suscriptor para el cual la AR ha remitido el requerimiento.	
En caso de renovación de un certificado, ANF AC genera y firma una nueva instancia del certificado, que difiere del anterior sólo por el período de validez y la firma de la Entidad de Certificación únicamente, siempre que ANF AC haya aprobado el requerimiento de renovación del certificado según lo especificado en el capítulo respectivo.	ISO 15782-1 7.3.3.9
En caso de re-emisión de un certificado, ANF AC genera y firma un nuevo certificado únicamente si la Entidad de Certificación ha aprobado el requerimiento de re-emisión según lo establecido en el capítulo respectivo.	ISO 15782-1 7.3.3.9
ANF AC notifica a la entidad solicitante cuando el certificado es emitido.	ISO 15782-1 7.3.3.6

v. Distribución de certificados

Objetivos de control. ANF AC tiene que mantener controles que proveen un nivel razonable de seguridad con relación a que, luego de la emisión, se pongan a disposición de los suscriptores y usuarios certificados adecuados y completos, de acuerdo con las prácticas de la Entidad de Certificación.

Procedimientos de control	Referencias
Distribución de certificados	
ANF AC pone los certificados que emite a disposición de los usuarios utilizando un mecanismo preestablecido (ej.: un repositorio) de acuerdo a su CPS y CP's en vigor.	X9.57 E.2 ISO 15782-1 7.3.6
Luego de la emisión, ANF AC incluye el certificado en el repositorio o utiliza otro mecanismo adecuado de distribución de acuerdo a su CPS y CP's de ANF AC.	X9.57 E.2 ISO 15782-1 7.3.6
Solo personal autorizado de ANF AC puede administrar su repositorio o el mecanismo de distribución alternativo.	
El funcionamiento del repositorio de ANF AC o del mecanismo de distribución alternativo es administrado y monitoreado.	

Se mantiene la integridad del repositorio de ANF AC o del mecanismo de distribución alternativo.	
--	--

vi. Revocación de certificados

Objetivos de control. ANF AC implementa controles que aseguran razonablemente que los certificados son revocados basados en solicitudes de revocación autorizadas y válidas.

Procedimientos de control	Referencias
Revocación de certificados	
De acuerdo a lo que establece su CPS, ANF AC provee un medio de rápida comunicación para facilitar la revocación segura y autenticada de: <ul style="list-style-type: none"> a) Uno o más certificados de una o varias entidades. b) El conjunto de todos los certificados emitidos por la Entidad de Certificación, utilizando un único par de claves. c) El conjunto de todos los certificados emitidos por la Entidad de Certificación, independientemente del par de claves utilizado para su emisión. 	ISO 15782-1 7.3.8.3 X9.57 4.6.1
ANF AC verifica o requiere que la AR verifique la identidad de la entidad solicitante de la revocación de un certificado y su autoridad para efectuar la petición, de acuerdo la CPS y CP asociada.	ISO 15782-1 7.3.8.3 X9.57 4.6.1
Si una AR externa acepta requerimientos de revocación, ANF AC requiere de la AR que envíe dichos requerimientos a la EPSC en forma autenticada, de acuerdo con la CPS y CP asociada.	ISO 15782-1 7.3.8.3
Si una AR externa acepta requerimientos de revocación y los reenvía a ANF AC, ésta provee un reconocimiento autenticado de la recepción del requerimiento a la UR, de acuerdo con la CPS y CP asociada.	ISO 15782-1 7.3.8.3
ANF AC actualiza la base de datos de certificados revocados y otros mecanismos referidos al estado de los certificados al efectuar una revocación, de acuerdo con la CPS y CP asociada.	X9.57 4.6.2.b
ANF AC registra todos los requerimientos de revocación de certificados y su seguimiento en un registro de eventos.	ISO 15782-1 7.3.8.3 X9.57 4.6.2.b
ANF AC o la AR proveen un aviso de revocación autenticado a la entidad cuyo certificado ha sido revocado, de acuerdo a lo establecido en la CPS y CP asociada.	ISO 15782-1 7.3.8.3
En caso de admitirse la renovación de un certificado, cuando el certificado es revocado todas las instancias válidas del mismo también lo son.	ISO 15782-1 7.3.8.3

vii. Suspensión de certificados

Objetivos de control. ANF AC tiene que mantener controles que permiten asegurar razonablemente que los certificados son suspendidos en base a solicitudes de suspensión autorizadas y válidas.

Procedimientos de control	Referencias
Suspensión de certificados	
De acuerdo a lo que establece la CPS, ANF AC provee un medio de rápida comunicación para facilitar la suspensión segura y autenticada de: <ul style="list-style-type: none"> a) Uno o más certificados de una o varias entidades. b) El conjunto de todos los certificados emitidos por la Entidad de Certificación, utilizando un único par de claves. c) El conjunto de todos los certificados emitidos por la Entidad de Certificación, independientemente del par de claves utilizado para su emisión. 	ISO 15782-1 7.3.8 X9.57 4.6.1
ANF AC verifica o requiere que las ARs externas verifiquen la identidad de la entidad solicitante de la suspensión de un certificado y su autoridad para efectuar tal solicitud, de acuerdo con las practicas de certificación publicadas y en vigor de la EPSC.	ISO 15782-1 7.3.8.3 X9.57 4.6.1
Si una AR acepta requerimientos de suspensión, la AR envía dichos requerimientos a la EPSC de manera que puedan ser autenticados, de acuerdo con la CPS y CP asociada.	ISO 15782-1 7.3.8.3
ANF AC o la AR notifican al suscriptor en caso de suspensión de un certificado.	ISO 15782-1 7.3.8.3 RFC 2527 4.2.1.1 X9.79 A
Los requerimientos de suspensión de certificados se procesan y validan de acuerdo a los requerimientos de la CPS y CP asociada.	RFC 2527 4.4.4.6 X9.79 A
ANF AC actualiza las CRL's luego de la suspensión de un certificado	X9.57 4.6.2.b
Los certificados son suspendidos solamente por el lapso de tiempo admitido en la CPS y CP asociadas de ANF AC.	RFC 2527 4.4.4.8 X9.79 A

Una vez que un certificado ha sido suspendido, dicha suspensión se gestiona de acuerdo con alguno de los mecanismos siguientes: a) Se ingresa un registro del certificado suspendido en la CRL, lo que obligará a los usuarios a rechazar las transacciones producidas durante el período de suspensión. b) El registro del certificado suspendido en la CRL se reemplaza por un registro de revocación del mismo certificador c) El certificado suspendido es restablecido nuevamente y su registro eliminado de la CRL.	X9.57 5.7.2
Un registro de suspensión del certificado permanece en la CRL hasta la expiración del mismo o hasta el vencimiento de su período de suspensión, lo que ocurra primero.	X9.57 5.7.2
ANF AC actualiza la CRL y otros mecanismos referidos al estado de los certificados luego de levantar una suspensión, de acuerdo con las prácticas de certificación publicadas y en vigor de la EPSC.	X9.57 4.6.2
ANF AC verifica o requiere que una AR externa verifique la identidad de la entidad que requiere el levantamiento de la suspensión de un certificado y su autoridad para efectuar tal requerimiento.	ISO 15782-1 7.3.8.3
Las suspensiones de certificados y su levantamiento o terminación se asientan en un registro de eventos.	ISO 15782-1 7.3.8.3 x9.57 4.6.2.b

viii. **Procesamiento de la información del estado de los certificados**

Objetivos de control. ANF AC tiene que mantener controles que aseguren razonablemente que se pongan a disposición de los suscriptores y usuarios información oportuna, completa y adecuada referida al estado de los certificados (incluida CRL y otros mecanismos referidos al dicho estado), de acuerdo a las prácticas de la PKI de ANF AC.

Procedimientos de control	Referencias
Procesamiento de información sobre el estado de los certificados	
La información sobre el estado de los certificados se encuentra disponible para todas las entidades relevantes.	ISO 15782-1 7.3.8.3
ANF AC pone a disposición de los usuarios la información sobre el estado de los certificados utilizando un mecanismo adecuado (ej.: CRL, OCSP) de acuerdo con las prácticas de certificación publicadas y en vigor de la EPSC.	ISO 15782-1 7.3.8.1

ANF AC firma digitalmente cada CRL que emite de manera tal que todas las entidades puedan validar su integridad y la fecha de su emisión.	ISO 15782-1 7.3.8.1
ANF AC emite CRL's periódicamente a intervalos regulares, según lo especificado en su CPS y CP's asociadas, aún cuando no se hubieran producido modificaciones desde la última emisión.	ISO 15782-1 7.3.8.1
Como mínimo, el registro de la CRL que identifica un certificado revocado permanece en la CRL hasta que finalice el período de validez del certificado o de acuerdo a lo establecido en las prácticas de certificación publicadas y en vigor de la EPSC.	ISO 15782-1 7.3.8.1 x9.57 4.6.2b
Si se admite la suspensión de certificados, un registro de la suspensión, con sus datos originales y de expiración permanecen en la CRL hasta la expiración normal del certificado, o de acuerdo a lo establecido en la CPS y CP's de ANF AC.	X9.57 4.6.2b
Las CRL's se archivan de acuerdo con los requerimientos de la CPS y a las normas vigentes.	ISO 15782-1 7.3.8
ANF AC incluye una secuencia numérica incremental para cada CRL emitida por ella (ej.: 1,2,3, etc.)	ISO 15782-1 9.2.3
La CRL contiene registros para todos los certificados revocados no expirados emitidos por ANF AC.	ISO 15782-1 9.2.4
Las CRL's anteriores son conservadas por el período de tiempo apropiado indicado en la CPS y CP's emitidas por ANF AC.	ISO 15782-1 7.3.8 X9.57 4.6.1
En caso de expiración, revocación, renovación, o suspensión de certificados, se conservan copias de los mismos por el período de tiempo apropiado, indicado en las normas vigentes de ANF AC, CPS y CP's.	
Si se utiliza un mecanismo de verificación del estado de los certificados en línea (ej.: OCSP), la EPSC requiere que las consultas sobre dicho estado contengan todos los datos requeridos por la CPS y CP's de ANF AC.	RFC 2560 2.1
Ante la recepción de una consulta sobre el estado de los certificados (ej.: consulta de OCSP) por parte de un usuario, la ANF AC dará una respuesta definitiva al usuario si: a) El mensaje de consulta se efectuó en forma correcta. b) La respuesta está configurada de manera de proveer el servicio requerido; y, c) La consulta contiene la información requerida según se establece en ANF AC.	RFC 2560 2.1

Todos los mensajes de respuesta definitiva son firmados digitalmente, de acuerdo con lo establecido en la CPS y CP's de ANF AC.	RFC 2560 2.2
Los mensajes de respuesta definitiva incluyen todos los datos requeridos de acuerdo con lo establecido en la CPS y CP's de ANF AC.	RFC 2560 2.2
Todos los mensajes de respuesta definitiva son firmados digitalmente, de acuerdo Si no se cumple cualquiera de las condiciones indicadas en este documento, ANF AC emite un mensaje de error, que puede estar o no firmado, según lo establecido en la CPS y CP's de ANF AC.	RFC 2560 2.1

ix. Administración del ciclo de vida de dispositivos externos de circuitos integrados (Integrated Circuit Cards, en adelante dispositivos)

Objetivos de control. ANF AC tiene que mantener controles que garanticen razonablemente la gestión segura del ciclo de vida de dispositivos externos de circuito integrado que aseguren razonablemente que:

- a) La preparación de los dispositivos es controlada por ANF AC en forma segura;
- b) Los archivos de datos de aplicación de los dispositivos son controlados en forma segura por ANF AC;
- c) La utilización de los dispositivos es habilitada por la ANF AC en forma previa a su emisión;
- d) Las tarjetas son almacenadas en forma segura y distribuidas por la ANF AC;
- e) La desactivación y reactivación de las tarjetas son controladas en forma segura por ANF AC, mediante protección multifactorial que combine enfoques físicos y lógicos; y,
- f) Se finaliza en forma segura el uso de las tarjetas devueltas a la Entidad de Certificación.

Procedimientos de control	Referencias
Nota: A efectos de esta sección, "circuito de tarjetas inteligentes" (SmartCards) incluyen dispositivos que pueden contener la clave privada de un suscriptor y un certificado.	
Preparación del circuito	
ANF AC como emisor de la tarjeta carga el Master File previa su distribución. ANF AC, controla posteriormente la personalización (la carga de archivos de datos y sus claves criptográficas) a través de software criptográfico específico, que garantiza al poseedor plena capacidad e independencia para la generación de su par de claves	ISO 10202-1 5.2.1
Tan solo los datos que identifican el circuito, al emisor de la tarjeta y a su poseedor son almacenados por ANF AC. ANF AC efectúa su activación, como emisor de la tarjeta, utilizando un proceso de control seguro.	ISO 10202-1 5.2.1 y 5.5.2

Luego de la activación de los datos, la tarjeta indica su estado de activación y protección.	ISO 10202-1 5.2.2
ANF AC registran la personalización de la tarjeta y el estado de activación de los datos. Preparación del archivo de datos de aplicación.	
Los datos específicos de la aplicación del proveedor almacenados en la tarjeta se localizan en el archivo de datos de aplicación. Esta localización (áreas de memoria en una tarjeta) es controlada en forma segura por ANF AC, como emisora de la tarjeta.	
ANF AC, como proveedora de la aplicación, controla la personalización del archivo de datos de la aplicación.	ISO 10202-1 5.3.1 y 5.3.2
ANF AC, como emisora de la tarjeta, utilizando un proceso de control seguro, ejecuta la activación del archivo de datos de la aplicación.	ISO 10202-1 5.3.3
Sólo puede activarse el archivo de datos de la aplicación cuando la tarjeta haya sido personalizada y activada o reactivada.	ISO 10202-1 5.3.3
Luego de la activación del archivo de datos de la aplicación, la tarjeta indica el estado de activación de los mismos.	ISO 10202-1 5.3.3
ANF AC registra la localización, personalización y activación del archivo de datos de la aplicación.	
Utilización del circuito	
Una tarjeta no es activada a menos que la misma haya sido personalizada.	ISO 10202-1 5.4.1
No es posible utilizar la tarjeta a menos que haya sido personalizada y se encuentre en un estado de activación o reactivación.	ISO 10202-1 5.4.1
Las tarjetas son almacenadas en forma segura, previo a su distribución.	
La recepción, activación y distribución de las tarjetas son registradas en un registro de eventos. Se mantiene un inventario de tarjetas y de su estado.	
Las tarjetas se distribuyen en forma segura. Desactivación del archivo de datos de la aplicación y del archivo de personalización.	

La desactivación del archivo de aplicación de datos puede ser efectuada únicamente por ANF AC, como proveedor de la aplicación.	ISO 10202-1 5.5.1
La desactivación del archivo de personalización puede ser efectuada únicamente por ANF AC, como emisora de la tarjeta.	ISO 10202-1 5.4.3
La reactivación del archivo de personalización se lleva a cabo bajo el control de ANF AC, como emisora de la tarjeta.	ISO 10202-1 5.4.3
La reactivación del archivo de aplicación de datos es conducida bajo el control de ANF AC, como proveedora de la aplicación.	ISO 10202-1 5.4.2
Son registradas tanto la desactivación y reactivación del archivo de aplicación de datos, como la desactivación y reactivación del archivo de personalización.	
Finalización del uso de la tarjeta	
ANF AC, como proveedor de la aplicación, controla la finalización del uso del archivo de datos de la aplicación.	ISO 10202-1 5.5.1
La finalización del uso del archivo de personalización es controlada por ANF AC, como emisora de la tarjeta.	ISO 10202-1 5.5.2

IV.d Controles sobre el estado de la técnica

i. Falsificación de certificados

Objetivos de control. ANF AC tiene que mantener controles que provean razonable seguridad contra la falsificación de certificados.

Procedimientos de control	Referencias
Trust Clonation	
ANF AC utiliza dispositivos que están protegidos contra la falsificación de certificados, especialmente contra el ataque conocido como "Confianza en la Clonación "Clonation Trust".	Trust Clonación

ii. Ataques al componente TOE

Objetivos de control. ANF AC tiene que mantener controles que provean razonable seguridad para impedir que los datos que el usuario manda al TOE puedan ser manipulados maliciosamente.

Procedimientos de control	Referencias
---------------------------	-------------

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 50 de 66

Falsificación del componente CSP	
ANF AC utiliza dispositivos que están protegidos contra la falsificación del módulo criptográfico para las operaciones de firma "CSP". Ataque conocido "Trust NSA" ANF AC debe de impedir debilidades en el modulo criptográfico que permita la creación de firmas falsas que no sean detectables por el sistema de verificación.	CWA-14167-2 3.3.1 T.Data Manipul T.Sign. Forgery
Falsificación del manejador de SmartCard	
ANF AC utiliza dispositivos que están protegidos contra la falsificación del manejador de las SmartCard. Ataque conocido "Trust Winscard"	CWA-14167-2 3.3.1 T.Data Manipul
Falsificación de los mandos de inicialización	
ANF AC debe de impedir que sean sustituidos los dispositivos de su entorno de certificación. Debe de controlar que el proceso de inicialización sea seguro.	CWA-14167-2 3.3.1 T.Insecure Init
Falsificación de los mandos durante la actualización del software	
ANF AC debe de impedir que sean sustituidos maliciosamente los dispositivos durante los procesos de actualización.	CWA-14167-2 3.3.1 T.Bad SW
Uso indebido de los datos de generación de firma	
Los datos de generación de firma son el recurso más valioso que el TOE debe de proteger. ANF AC debe disponer de controles que solo permitan su uso legitimo al ser derivados de alguna forma maliciosa.	CWA-14167-2 3.3.1 T-CSP-SCD derive
Decubrimiento de los datos de generación de firma	
ANF AC debe de proteger los datos de generación de firma contra cualquier ataque que puede presuponer su descubrimiento total o parcial.	CWA-14167-2 3.3.1 T-CSP-SCD disclose
Uso de certificados revocados	
ANF AC debe de impedir el uso de certificados cuya seguridad se ha quebrantado.	CWA-14167-2 3.3.1 T-CSP-SCD distortion
Funcionamiento defectuoso del TOE	

ANF AC debe de impedir que un funcionamiento defectuoso del TOE ya sea fortuito o provocado, permita descubrir o distorsionar los datos de generación de firma, los datos a firmar o cedan maliciosamente los mandos del TOE.	CWA-14167-2 3.3.1 T-Malfunction
Funcionamiento del TOE en un ambiente inseguro	
ANF AC debe de impedir que el TOE pueda conectarse a un sistema hostil.	CWA-14167-2 3.3.1 T-Insecure Oper
Modificación de los datos del usuario por personal de la CSP	
ANF AC debe de impedir la posibilidad de que su personal pueda manipular los datos del usuario.	CWA-14167-2 3.3.1 T-Management
Mal uso de la Firma	
ANF AC debe de impedir la posibilidad de un mal uso de la firma que permita crear certificados o falsear la información del estado de los certificados.	CWA-14167-2 3.3.1 T-Misuse Sign
Manipulación física del TOE	
ANF AC debe de impedir la posibilidad de la manipulación física del TOE.	CWA-14167-2 3.3.1 T-Phys Manipul
Sustracción de TOE	
El robo de todo o parte del TOE puede producir una pérdida de la confidencialidad o integridad y/o la disponibilidad del sistema.	CWA-14167-2 3.3.1 T-Theft

iii. Tecnología Grid

Objetivos de control. ANF AC tiene que mantiene un control de seguimiento del resultado de la tecnología Grid.

Procedimientos de control	Referencias
Tecnología eGrid	

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 52 de 66

ANF AC mantiene un seguimiento de los resultados obtenidos por la Tecnología eGrid y su posible aplicación a “public key cryptography”.

eGrid

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 53 de 66

V. Controles del Sistema de ANF AC

Los objetivos y procedimientos de control que se describirán a continuación representan los criterios mínimos a los que se deberá ajustar ANF AC para ejercer su actividad como entidad prestadora de servicios de certificación.

Estos criterios están basados en la Norma ISO 17799/UNE 717799, de Gestión de Seguridad de la Información que en su capítulo 12, aunque no únicamente, recoge las normas legales que una organización debe de contemplar, y que constituyen el eje del denominado Derecho de las Tecnologías de la Información.

Los mecanismos, procesos y objetivos de control referenciados se orientan a evaluar y establecer la situación de ANF AC en relación con estas normas legales. La adecuación de su entorno tecnológico a estas normas, en especial a la aplicación que se realiza de los datos de generación de firma vinculados a los certificados que esta CA emite, y las características de los dispositivos seguros de creación y verificación de firma electrónica que ANF AC ha homologado.

Los objetivos de control han sido agrupados en tres secciones. En todas ellas el auditor debe realizar aquellas pruebas sustantivas y de cumplimiento que le permitan verificar la existencia, el cumplimiento y la eficacia de los procedimientos de control implementados. Debe de revisar las prácticas, las políticas y los manuales de publicados por ANF AC, y asegurarse que los mismos son conocidos y aplicados por el personal correspondiente. Las pruebas podrán incluir revisiones de la documentación, utilización de software específico de auditoría, de programas utilitarios adecuados para la revisión, así como inspecciones oculares y entrevistas al personal y todo otro procedimiento que juzgue conveniente.

A continuación se presentan los criterios mínimos de cada sección, los cuales deben de interpretarse como una guía, respecto a los objetivos y procedimientos de control que deben estar implementados por ANF AC. Resulta esencial que el auditor utilice su juicio profesional para determinar la naturaleza, el alcance y la oportunidad de las pruebas de auditoría a realizar, con el fin de emitir una opinión sobre el ambiente de control interno y el cumplimiento del marco normativo aplicable.

V.a Elementos del Sistema

I Interpretación de las definiciones

Objetivos de control. Las definiciones recogidas en las prácticas de certificación de ANF AC, deben de garantizar una correcta interpretación de acuerdo con el marco legal:

- a) Firma Electrónica Avanzada.
- b) Firma Electrónica Reconocida.
- c) Certificado Reconocido.
- d) Dispositivo Seguro de Creación de Firma.
- e) Dispositivos de Verificación de Firma electrónica
- f) Sellos de Tiempo
- g) Autoridad de Sellos de Tiempo (TSA)

Procedimientos de control	Referencias
---------------------------	-------------

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 54 de 66

Definiciones de Firma Electrónica	
<p>La Firma Electrónica Avanzada es aquella que:</p> <ul style="list-style-type: none"> a) que esta vinculada al firmante de manera única y a los datos a los que se refiere; b) es capaz de identificar al firmante c) permite detectar cualquier cambio ulterior de los datos firmados; y d) y que ha sido creada por medios que el firmante mantiene bajo su exclusivo control 	<p>Dir.1999/93/CE Ley 59/2003 CWA 14167-1</p>
<p>Se define como Firma Electrónica Reconocida la Firma Electrónica Avanzada que:</p> <ul style="list-style-type: none"> a) este basada en un certificado reconocido; b) es generada mediante un dispositivo seguro de creación de firma. 	<p>Ley 59/2003</p>
Certificado Reconocido	
<p>Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en Ley 59/2003 en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten medios admitidos en derecho.</p>	<p>Dir.1999/93/CE Anexo II Ley 59/2003 CWA 14167-1</p>
Dispositivo Seguro de Creación de Firma	
<p>Es el dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:</p> <ul style="list-style-type: none"> a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto. b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento. c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros. d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma. 	<p>Ley 59/2003 Dir.1999/93/CE Anexo III CWA 14167-1</p>
Dispositivo de Verificación de Firma	
<p>Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.</p>	<p>Ley 59/2003 Dir.1999/93/CE Anexo III CWA 14167-1</p>
Sellos de Tiempo	
<p>Sellos de Tiempo: Es el conjunto de valores que habiendo vinculado unos datos a un tiempo determinado, representan una evidencia de que esos datos existieron antes de ese tiempo.</p>	<p>CWA 14167-1</p>

<p>Auditoría del Estado del Certificado <i>Servicio de Sellos de Tiempo</i> Una Autoridad de Sellos de Tiempo (TSA) es una tercera parte confiable que proporciona el sello de tiempo.</p>	<p>CWA 14167-1 RS3 5.3.1</p>
--	-----------------------------------

V.b Requerimientos

Objetivos de control. Determinar que los dispositivos empleados por ANF AC y el producto resultante al aplicarlos cumple con los requerimientos establecidos por las normas aplicables al efecto.

Procedimientos de control	Referencias
Firma Electrónica	
<p>Firma Electrónica Avanzada debe de cumplir con los siguientes requisitos:</p> <ul style="list-style-type: none"> a) que esta vinculada al firmante de manera única y a los datos a los que se refiere; b) es capaz de identificar al firmante c) permite detectar cualquier cambio ulterior de los datos firmados; y d) y que ha sido creada por medios que el firmante mantiene bajo su exclusivo control 	<p>Dir.1999/93/CE Ley 59/2003 CWA 14167-1</p>
<p>La Firma Electrónica Reconocida debe de cumplir con los siguientes requisitos:</p> <ul style="list-style-type: none"> a) tratarse de una Firma Electrónica Avanzada; b) que este basada en un certificado reconocido; y c) generada mediante un dispositivo seguro de creación de firma. 	<p>Ley 59/2003</p>
Certificado Reconocido	
<p>Los certificados reconocidos emitidos por ANF AC incluyen como mínimo:</p> <ul style="list-style-type: none"> a)La indicación de que se expiden como tales. b)El código identificativo único del certificado. c)La identificación del prestador de servicios de certificación que expide el certificado y su domicilio. d)La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado. e)La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal. f)Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante. g)El comienzo y el fin del período de validez del certificado. h)Los límites de uso del certificado, si se establecen. i)Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen. 	<p>Ley 59/2003</p>

Dispositivo Seguro de Creación de Firma	
<p>El dispositivo seguro de creación de firma homologado por ANF AC ofrece, al menos, las siguientes garantías:</p> <ul style="list-style-type: none"> a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto. b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento. c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros. d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma. 	<p>Ley 59/2003 Dir.1999/93/CE Anexo III CWA 14167-1</p>
Dispositivo de Verificación de Firma	
<p>Los dispositivos de verificación de firma electrónica homologados por ANF AC garantizarán, garantizan al menos, los siguientes requisitos:</p> <ul style="list-style-type: none"> a) Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma. b) Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente. c) Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados. d) Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación. e) Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente. f) Que pueda detectarse cualquier cambio relativo a su seguridad. 	<p>Ley 59/2003 Dir.1999/93/CE Anexo III CWA 14167-1</p>
Sellos de Tiempo	
<p>La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.</p>	<p>Ley 59/2003</p>

<p><i>Servicio de Sellos de Tiempo</i></p> <p>Requisitos funcionales</p> <ul style="list-style-type: none"> • <i>Exactitud de Demanda del Sello</i> <p>Este componente se diseña para verificar la exactitud y la integridad de la petición. Si el resultado es positivo, los datos se envían como entrada del sello.</p> <ul style="list-style-type: none"> • <i>Generación de Parámetro de Tiempo</i> <p>Se utiliza una fuente fiable de tiempo para crear los parámetros correspondientes al tiempo actual..</p> <ul style="list-style-type: none"> • <i>Generación del Sello de Tiempo</i> <p>Esta función es responsable de crear un sello de tiempo vinculando el tiempo actual, a los datos y a un identificador único.</p> <ul style="list-style-type: none"> • <i>El Cómputo de Ficha de Time-estampa</i> <p>Este componente computa la ficha del sello de tiempo que se devuelve al cliente.</p>	<p>CWA 14167-1 RS3.1 5.3.1.1</p>
<p>Exactitud de la Petición</p> <p>El TSA puede controlar el origen de cada petición antes de verificar su exactitud.</p>	<p>CWA 14167-1 RS3.1 5.3.1.2 TS1.1</p>
<p>El reloj del TSA se sincronizará con UTC</p>	<p>CWA 14167-1 RS3.1 5.3.1.2 TS2.2</p>
<p>El número de serie usado dentro del sello de tiempo debe ser único para cada sello emitido por un TSA.</p> <p>Esta propiedad incluso debe conservarse después de una posible interrupción</p>	<p>CWA 14167-1 RS3.1 5.3.1.2 TS3.1</p>

V.c Normativa legal

Objetivos de control. Determinar que ANF AC ha atendido todos los aspectos legales derivados de la actividad que desarrolla en el territorio español.

Procedimientos de control	Referencias
Ley de Firma Electrónica	
Los prestadores de servicios de certificación que expidan certificados electrónicos deben cumplir obligaciones determinadas en este artículo.	Ley 59/2003 Art. 18
La Firma Electrónica Reconocida debe de cumplir con los siguientes requisitos: a) tratarse de una Firma Electrónica Avanzada; b) que este basada en un certificado reconocido; y c) generada mediante un dispositivo seguro de creación de firma.	Ley 59/2003 Art. 20
Los prestadores de servicios de certificación deberán comunicar al Ministerio de Ciencia y Tecnología el inicio de su actividad.	Ley 59/2003 Art. 30

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 58 de 66

Ley de servicios de la sociedad de la información y de comercio electrónico.	
Constancia registral del nombre de dominio.	Ley 34-2002 Art. 9
Información general	Ley 34-2002 Art. 10
Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.	Ley 34-2002 Art. 12
Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios.	Ley 34-2002 Art. 15
Ley Orgánica de Protección de Datos de Carácter Personal	
Establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal	R.D. 994/1999 LOPD 15/1999
Ley Propiedad Intelectual	
Cumplimiento de la normativa de Propiedad Intelectual.	Basado en el R.D. 1/1996
Derecho Laboral	
Todas aquellas normas que tengan relación con la regulación y limitación del uso por parte de los empleados de ANF AC de sus sistemas de tratamiento de la información.	Basado en el R.D. 2/1995
Derecho Procesal	
En todas aquellas normas que estén relacionadas con la aptitud de la información en formato digital, para ser objeto de prueba en un procedimiento judicial y condiciones y requisitos para tal fin.	Basado en el Ley 1/2000

VI. Siglas

ANS	American National Standard Institute.
AR	Autoridad de Registro.
CARAT	Certification Authority Rating and Trust Guidelines.
CPS	Declaración de Prácticas de Certificación. "Certification Practice Statement"
CP's	Políticas de Certificación. "Certificate Policy".
CRL's	Listas de Certificados Revocados
CSP	Proveedor de Servicios de Certificación. "Certification-service-provider"
EPSC	Entidad Prestadora de Servicios de Certificación = CSP
FIPS	Federal Information and Processing Standard.
IETF	Internet Engineering Task Force.
ISO	International Organization for Standardization.
ITU	International Telecommunications Union.
NIST	National Institute of Standards and Technology.
OID	Object Identifier.
PKI	Infraestructura de Clave Pública. "Public Key Infrastructure"
SCD	Datos de Creación de Firma. "Signature Creation Data"
SVD	Datos de Verificación de Firma. "Signature Verification Data"
TOE	Módulo criptográfico del CSP-SCD y para la creación de firmas avanzadas.
TSA	Autoridad de Sellos de Tiempo. "Time-Stamping Authority"
URL	Dirección de Internet. "Uniform Resource Locator"

VII. Orígenes y objetivos de los principales estándares contemplados en este documento.

ANSI 9.79:2001.

Este Estándar, aprobado en enero de 2001 por el Instituto Americano de Estándares Nacionales (American National Standard Institute, ANSI), se refiere al Marco de Prácticas y Políticas de las Infraestructuras de Claves Públicas (PKI Practices and Policy Framework, por sus siglas en inglés). Aunque originariamente elaborado para atender las necesidades de las entidades financieras (concretamente de la American Bankers Association, PKI Practices and Policy Framework American -PKI Practices and Policy Framework, American-), su uso puede ser adaptado y extendido a otras organizaciones. Su Anexo A establece los componentes de una Política de Certificación y de un Manual de Procedimientos de Certificación, mientras que su Anexo B detalla los objetivos de control de las EPSC. Sus anexos C y E se refieren a las extensiones de los certificados X.509 y los identificadores de objetos (OID).

El objetivo del estándar es atender las necesidades de gerentes y analistas de negocios interesados en la tecnología de ICP, diseñadores e implementadores técnicos y auditores y gerentes de operación.

En la actualidad, este estándar de la ANSI está siendo revisado para su incorporación futura como la norma ISO 21188 sobre políticas y prácticas de PKI.

ISO 17799

Basado originalmente en la Norma 17799 del Instituto Británico de Estándares (British Standard Institute), este constituye un código de práctica para la gestión de la seguridad de la información. Fue emitido por la Organización Internacional para la Estandarización (International Organization for Standardization-ISO). Contiene recomendaciones aplicables por los responsables de iniciar, implementar o mantener aspectos de seguridad en las organizaciones. Provee una base común para el desarrollo de políticas y procedimientos de seguridad y de prácticas efectivas de administración de la misma, promoviendo la confianza en las relaciones entre entidades. Es una de las referencias más importantes a la hora de analizar aspectos de seguridad de ambientes computarizados. Esta norma se especifica en 12 elementos:

1. Alcance,
2. Términos y Definiciones,
3. Política de Seguridad,
4. Organización de la Seguridad,
5. Clasificación y Control de Activos,
6. Seguridad del Personal,
7. Seguridad Ambiental y Física,
8. Gestión de Comunicaciones y Operaciones,
9. Control de Accesos,
10. Desarrollo y Mantenimiento del Sistema,
11. Administración de la Continuidad de los Negocios,
12. Conformidad/Cumplimiento.

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 61 de 66

RFC 2527

Constituye un documento de trabajo del Grupo de Trabajo de PKI (PKIX Working Group), del Grupo de Tareas de Ingeniería de Internet (Internet Engineering Task Force – IETF). Este documento, el cual está siendo revisado en la actualidad, presenta un marco para asistir a los responsables de la redacción de políticas y procedimientos de certificación aplicables a PKI. Particularmente, lista, en forma detallada, una serie de asuntos a contemplar en una CPS y CP's.

ISO 15782-1

Este documento, al igual que el ANS9.79, surge como respuesta a necesidades específicas del sector financiero, pero los conceptos a los que hace referencia son aplicables a otras áreas. Aún en etapa de revisión, fue redactado por la ISO y se refiere a la administración de los certificados digitales para el sistema bancario.

X9.57

Este estándar, publicado en 1997 por la ANSI, se refiere a la Administración de certificados en el campo de la criptografía de clave pública para la industria de los servicios financieros.

ISO 10202-1

Este estándar fue publicado por la ISO en 1991, y se refiere a las tarjetas de transacciones financieras. Específicamente trata la arquitectura de seguridad para los sistemas transaccionales de entidades financieras, que emplean tarjetas de circuitos integrados. En su parte 1, se refiere al ciclo de vida de las tarjetas.

FIPS 140-1

Este documento es un Estándar para el procesamiento de información federal del gobierno de los EEUU, y se refiere a los requerimientos de seguridad para los módulos criptográficos. Fue emitido en 1993. Esta norma tiene como característica la utilización de elementos de hardware revestidos con resinas epoxídicas y los sellos resistentes a las manipulaciones indebidas.

CARAT

La sigla responde a la denominación del documento llamado “Confiabilidad y Ranqueo de Autoridades de Certificación: Guías para la construcción de Políticas relativas al uso de certificados de clave pública basados en la identidad” (Certification Authority Rating and Trust: guidelines for constructing Policies Governing the Use of Identity based Public Key Certificates). Fueron emitidos por la National Automated Clearing House Association (NACHA).

ISO 9594/X.509

Recomendación de la ITU-T, de 1997, relativa a Tecnologías de la Información, Interconexiones en sistemas abiertos, marcos de autenticación para los directorios.

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 62 de 66

X9.30

Este estándar publicado en 1997 por el ANSI, se refiere a la criptografía de clave pública para la industria de los servicios financieros, y específicamente al Algoritmo de firma digital (Digital Signature Algorithm - DSA).

X9.31

El estándar ANS X9.31, de 1998, emitido por la ANS, se refiere a las firmas digitales utilizando criptografía de clave pública reversible (Reversible Digital Signature Algorithm - rDSA), para la industria de los servicios financieros.

X9.62

Este estándar, publicado por la ANS en 1998, se refiere a la criptografía de clave pública para la industria de los servicios financieros, y particularmente al Algoritmo de curvas elípticas para firma digital (Elliptic Curve Digital Signature Algorithm - ECDSA).

X9.82

Se trata de un documento en elaboración en el ANSI, relativo a la generación de números aleatorios para la emisión del par de claves criptográficas asimétricas.

X9.80

Este documento se encuentra aún en etapa de elaboración en el ANSI, y se refiere a la generación de números primos, a los tests de primalidad para verificación de su condición de números primos y a la certificación de primalidad.

ISO 11568

Este estándar de la ISO, fue publicado en 1998 y se orienta a las transacciones del sector bancario, aunque sus contenidos pueden ser adaptados a otros sectores. Describe los procesos de administración de claves. En su parte 4, se refiere a las técnicas de gestión de claves utilizando criptografía de clave pública. Otra de sus secciones, describe el ciclo de vida de las claves para los criptosistemas de clave pública.

ISO 13491-1

Se trata de un borrador bajo análisis en la ISO, relativo a los dispositivos criptográficos seguros. En su parte 2, contiene listas de chequeo (*checklists*) de cumplimiento de aspectos de seguridad para los dispositivos que utilizan sistemas de tarjetas de banda magnética. Fue publicado en julio de 1998.

CWA 14167-1 (Marzo 2003)

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 63 de 66

Requisitos de seguridad de sistemas fiables que controlan los certificados de firmas electrónicas —
Parte 1: Sistema de condiciones de seguridad.

Incluida en la lista de normas que gozan de reconocimiento general para productos de firmas electrónicas considerados conformes por los Estados miembros con los requisitos del anexo II (f) y III. En el mes de junio del año 2.003, la Comisión Europea decidió la publicación en el «Diario Oficial de la Unión Europea» de este número de referencia.

CWA 14167-2 (Marzo 2002)

Requisitos de seguridad de sistemas fiables que controlan los certificados de firmas electrónicas —
Parte 2: Módulo criptográfico para las operaciones de firmas CSP — Perfil de protección (MCSO-PP).

Incluida en la lista de normas que gozan de reconocimiento general para productos de firmas electrónicas considerados conformes por los Estados miembros con los requisitos del anexo II (f) y III. En el mes de junio del año 2.003, la Comisión Europea decidió la publicación en el «Diario Oficial de la Unión Europea» de este número de referencia.

CWA 14169 (Marzo 2002)

Dispositivos protegidos de creación de firma electrónica.”

Incluida en la lista de normas que gozan de reconocimiento general para productos de firmas electrónicas considerados conformes por los Estados miembros con los requisitos del anexo II (f) y III. En el mes de junio del año 2.003, la Comisión Europea decidió la publicación en el «Diario Oficial de la Unión Europea» de este número de referencia.

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 64 de 66

VIII. Bibliografía

- ANS X9.30:1997 – *Public Key Cryptography for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA) - American National Standard Institute.*
- ANS X9.31:1998 – *Digital Signatures Using Reversible Public Cryptography for the Financial Services Industry (rDSA) - American National Standard Institute.*
- ANS X9.57:1997 – *Public Key Cryptography for the Financial Services Industry: Certificate Management – American National Standard Institute.*
- ANS X9.62:1998 – *Public Key Cryptography for the Financial Services Industry: Certificate Management - American National Standard Institute.*
- ANS X9.66: DRAFT – *Cryptographic Device Security - American National Standard Institute.*
- ANS X9.79:2001 – *Part 1: PKI Practices and Policy Framework – American National Standards Institute.*
- ANS X9.80: DRAFT – *Prime Number Generation, Primality Testing, and Primality Certificates - American National Standard Institute.*
- ANS X9.82 – DRAFT – *Random Number Generation - American National Standard Institute.*
- CARAT – *Certification Authority Rating and Trust Guidelines : Guidelines for Constructing Policies Governing the Use of Identity Based Public Key Certificates – National Automated Clearing House Association (NACHA). Digital Signature Guidelines, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce – American Bar Association, Information Security Committee.*
- FIPS 140-1 – *Security Requirements for Cryptographic Modules – Federal Information Processing Standard.*
- ISO 10202-1:1991 – *Financial Transaction cards – Security architecture of financial transaction systems using integrated circuit cards – Part 1: Card life cycle – International Organization Institution.*
- ISO 11568-4:1998 – *Banking – Key Management (retail) – Part 4: Key Management Techniques using public key cryptography – International Organization for Standardization.*
- ISO 11568-5:1998 – *Banking – Key Management (retail) – Part 5: Key Life cycle for public key cryptosystems - International Organization for Standardization.*
- ISO 13491-1: DRAFT – *Banking – Secure Cryptographic Devices (Retail) – Part 2: Security Compliance Checklists for Devices used in Magnetic Stripe Card Systems - International Organization for Standardization.*
- ISO 15782-1: DRAFT – *Banking, Certificate Management Part 1: Certificate Management - International Organization for Standardization.*
- ISO 17799 - *Information technology – Code of practice for information security management - International Organization for Standardization.*

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 65 de 66

ISO 9594/X.509 *Public Key Infrastructure CP and Certification Practices Framework – IETF Request for Comments Draft. Online Certificate Status Protocol - IETF Request for Comments Draft*

PKI Assessment Guidelines – *American Bar Association, Information Security Committee.*

RFC 2527 – *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework - Network Working Group – PKIX.*

ANF AC	Ref. Normas y Criterios de Auditoría de los Servicios de Certificación	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.11.1	Página 66 de 66