AUTORIDAD DE CERTIFICACIÓN
ANF-AC CERTIFICATION AUTHORITY

Declaración de Prácticas de Certificación
ANF Server CA
(DPC)

Certificate Practice Statement
ANF Server CA
(CPS)

Fecha : 1 de enero de 2010
Versión : 1.0
OID : 1.3.6.1.4.1.18332.1.9

AUTORIDAD DE CERTIFICACIÓN
ANF-AC CERTIFICATION AUTHORITY

Declaración de Prácticas de Certificación de

ANF Autoridad de Certificación.

Sumario

1. Definiciones

A efectos de lo dispuesto en el presente documento, y únicamente cuando los términos comiencen con letra mayúscula y estén en cursiva, se entenderá por:

- *ANF AC :* Es ANF Autoridad de Certificación, entidad raíz de esta infraestructura de clave pública.
- *ANF AC TSA :* Corresponde al término utilizado por *ANF AC,* en la prestación de su servicio de sellado de tiempo, como Autoridad de Sellado de Tiempo.
- *ARR :* Es Autoridad de Registro Reconocida, ente colaborador del prestador de servicios de certificación, en el proceso de solicitud e identificación de los usuarios.
- *Autoridades Intermedias:* Son *PSC Subordinados* que bajo la jerarquía de los certificado raíz -ANF Root CA- y –ANF Clase 1 CA- emiten certificados a usuarios finales.
- *CEN :* Comité Européen de Normalisation
- *Certificado :* Es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. (*LFE 59/2003, Tit. II Cap. I Art. 6.1*)
- *CP :* Es la contracción del vocablo inglés “Certificate Policy” – en español Política de Certificación - . La Política de Certificación define los requerimientos específicos que deben de ser atendidos para la emisión y uso de un determinado certificado. Cada certificado de *ANF AC* se somete a una *CP* determinada.
- *CWA* : CEN Workshop Agreement
- *Datos de Creación de Firma:* En la *PKI* de *ANF AC* es la clave criptográfica asimétrica privada que el signatario utiliza para crear firmas electrónicas.
- *Datos de Verificación de Firma:* En la PKI de *ANF AC* es la clave criptográfica asimétrica pública que se utilizan para verificar las firmas electrónicas.
- *Dispositivo homologado de ANF AC* : Con el fin de establecer unas garantías homogéneas de seguridad técnica y jurídica, *ANF AC* pone a disposición de sus usuarios y entidades colaboradoras una serie de dispositivos sobre los que ha efectuado las comprobaciones necesarias de calidad. Estos dispositivos gozan de la calificación de homologados.
- *Dispositivo Seguro de Creación de Firma*: Es el dispositivo de creación de firma electrónica que cumple los requerimientos de la norma ISO 15408 Common Criteria EAL 4+.

- *Documento electrónico:* Es un conjunto de registros lógicos almacenado en un soporte que permite ser leído por equipos informáticos.
- *DPC* : Declaración de Prácticas de Certificación, en inglés - Certification Practice Statement (CPS)-. Define los procedimientos seguidos por *ANF AC* en la prestación de sus servicios de certificación, la *DPC* y su addenda, definen la *PKI* de *ANF AC*.
- *Función resumen:* También llamada función hash, es la aplicación de un algoritmo matemático a un documento electrónico, da como resultado un Hash vinculado unívocamente al documento electrónico. Los algoritmos más conocidos son MD5, SHA-1 y SHA-2, el primero de 1.991 y con una longitud de 128 bits, ya esta catalogado como "no seguro".
- *Hash* : Es un resultado de tamaño fijo que se obtiene tras aplicar una función hash a un documento electrónico. Su propiedad es básicamente que un mismo documento da siempre como resultado el mismo *Hash*, y documentos distintos dan como resultado *Hash* diferentes. Sobre esta característica se fundamente el atributo de Integridad de la Firma Electrónica. También es conocido el Hash por el nombre de "huella digital".
- *Hashing* : Es la aplicación de una función resumen, a un documento electrónico.
- *JRPKI* : Es la Junta Rectora de la PKI, encargada de supervisar y asesorar a *ANF AC*.
- *OID* : Es la contracción del vocablo inglés "Object Identifier Digital" – en español Identificador Digital de Objetos-. Es un valor de naturaleza jerárquica, siempre formador por enteros no negativos separados por un punto. En esta sistema de certificación son asignados a objetos registrados, y tiene la propiedad de ser únicos entre el resto de *OID*.
- *PKI* : Es la contracción del vocablo en inglés "Public Key Infrastructure" –en español Infraestructura de Clave Pública-. La PKI es el conjunto de entidades, procedimientos, dispositivos...etc., que conforman un sistema de certificación.
- *PSC* : Prestador de Servicios de Certificación, es la persona física o jurídica que en el ámbito de la legislación en materia de firma electrónica, expide los certificados electrónicos y presta servicios relacionados con la Firma Electrónica.
- *PSC Subordinados:* Son Autoridades Intermedias que bajo la jerarquía del certificado raíz -ANF Root CA- y –ANF Clase 1 CA- emiten certificados a usuarios finales.

- *RSA* : Acrónimo de - "Rivest, Shamir y Adleman". Inventores del criptosistema de clave pública que permite la firma electrónica y el cifrado (1977). Es el criptosistema de clave pública que permite la creación de una firma digital.
- *SHA*-1 : "Secure Hash Algorithm" (1994). Este algoritmo de resumen esta en situación de RIESGO. Genera un resumen de 160 bits. Hasta el presente es el algoritmo utilizado por la practica totalidad de prestadores de servicios de certificación, se emplea en "funciones resumen" (hash) que tienen como objetivo dotar de Integridad a los documentos electrónicos durante el proceso de firma.
- *SHA*-2 : En el sistema de certificación de *ANF AC,* este algoritmo esta llamado a sustituir al SHA-1 en aquellos procesos en los que aun se utiliza. Internacionalmente SHA-2 está clasificado como seguro.
- *SSL* : Contracción del vocablo inglés "Secure Socket Layer". Es el sistema, de uso común, para garantizar la privacidad de las comunicaciones y garantizar la identidad cierta del servidor al que se conecta.
- *TimeStamping*: Sellado Digital de Tiempo. *ANF AC* dispone de un servicio de fechado electrónico. Este servicio esta sometido a su propia *DPC* bajo la denominación de ANF AC TSA .
- *TSA*: Contracción del vocablo inglés "Time-Stamping Authority". Correspondiente al término Autoridad de Sellado de Tiempo, ANF AC TSA administra *TSS*.
- *TSS*: Contracción del vocablo inglés "time-stamp service". Corresponde al término servicio de sellado de tiempo, que emite *TST*.
- *TST*: Contracción del vocablo inglés "time-stamp token". Corresponde al sello digital de tiempo emitido por un servicio de sellado de tiempo desde un *TSU*.
- *TSU*: Contracción del vocablo inglés "time-stamp unit". Corresponde a una Unidad específica de sellado de tiempo, perteneciente a los *TSS* de la *TSA*. Es la unidad desde la que se crean y firman en nombre de la *TSA* los sellos digitales de tiempo.
- *UTC:* Contracción del vocablo inglés "Universal Co-ordinated Time" (anteriormente GMT). Corresponde al término "tiempo universal coordinado" y es el tiempo en el que se basó la emisión del "time-stam token" *TST*, definido en la Recomendación de ITU-R TF.460-5 [TF.460-5]

2. Introducción.

2.1 Presentación.

ANF Autoridad de Certificación, (*en adelante ANF AC*), es una entidad jurídica, constituida al amparo de la Ley Orgánica 1/2002 del 22 de marzo e inscrita en el Ministerio del Interior con el número nacional 171.443 y CIF G-63287510.

La denominación completa de este documento es *Declaración de Prácticas de Certificación* de *ANF AC* (*en adelante DPC*). Este término *DPC* se corresponde con el concepto inglés de Certification Practice Statement (*CPS*).

Esta *DPC* se ha inspirado en la norma RFC 3647 "*Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framewortk*" del Internet Engineering Task Force (IETF) (que sustituye a la RFC2527) como guía de asistencia en la redacción de este tipo de documentos. La *DPC* de *ANF AC* contempla todas las secciones esenciales de la especificación, e incluye otras secciones que, a juicio del autor, considera necesarias para una correcta adaptación a las exigencias del marco legislativo internacional.

2.2 Identificación.

Nombre del documento	Declaración de Prácticas de Certificación de ANF AC. "*DPC de ANF AC*"
Versión	2
Autor	*Florencio Díaz Vilches*
Referencia del documento / OID	1.3.6.1.4.1.18332.1.9
Fecha de emisión	1 de enero de 2010
Fecha de expiración	No es aplicable
Localización URL	https://www.anf.es/AC/documentos/
Ámbito de aplicación	Ver punto 2.5.4

ANF Autoridad de Certificación tiene asignado el código privado de empresa (SMI Network Management Private Enterprise Codes) **18332** por la organización internacional IANA -Internet Assigned Numbers Authority-, bajo la rama

iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 -IANA –Registered Private Enterprise-). Esto puede ser consultado en la URL:

http://www.iana.org/assignments/enterprise-numbers

El prefijo del *OID* de esta *DPC* es 1.3.6.1.4.1.18332.**1.** el sufijo es el **9**. En el caso de este documento, el *OID* que lo identifica es 1.3.6.1.4.1.18332.1.9

El protocolo a seguir en el mantenimiento de este *OID* queda determinado en el apartado "*Procedimiento de Especificación de Cambios*" de este documento.

2.3 Datos de contacto.

2.3.1 Especificación del ente organizador.

Esta *DPC* es propiedad de *ANF AC*:

ANF Autoridad de Certificación

NIF G-63287510
Gran Vía de les Corts Catalanes, 996
08018 - Barcelona - España
Tfno.- 00 34 932 661 614
FAX.- 00 34 933 031 611
Dirección electrónica: ac@anf.es
Dirección Web: http://www.anf.es/

Esta *DPC* esta administrada por la Junta Rectora de la PKI de *ANF AC*:

JRPKI de la ANF Autoridad de Certificación
Gran Vía de les Corts Catalanes, 996
08018 - Barcelona - España
Tfno.- 00 34 932 661 614
FAX.- 00 34 933 031 611
Dirección electrónica: juntapki@anf.es

2.3.2 Persona de contacto

Para cualquier información relacionada con esta *DPC*:

Persona de contacto: F. Díaz
e-Mail: fdiaz@anf.es

2.3.3 Adecuación de la *DPC* a las Políticas de Certificación

Las modificaciones propuestas o las nuevas aportaciones a incluir sobre esta *DPC*, deben, previa a su aprobación, ser contrastadas con las Políticas de Certificación (en adelante *CP*) y Políticas de Firma que *ANF AC* tenga publicadas, a fin de asegurar que DPC de ANF AC y las Políticas soportan estos cambios.

El procedimiento a seguir queda especificado en el apartado "*Seguridad de la adecuación de la DPC a las Políticas asociadas*" de este documento.

2.4 Publicación.

Este documento y anexos puede obtenerse libremente en la URL :

https://www.anf.es/ AC/documentos/,

o en las oficinas centrales de *ANF AC*.

La entidad con atribuciones para definir y aprobar sobre cualquier propuesta de modificación de esta *DPC* es la Junta Rectora de la PKI.

El mantenimiento y el control de la correcta aplicación de lo establecido en esta *DPC*, recae sobre la Dirección Ejecutiva de *ANF AC*.

2.5 Comunidad y ámbito de aplicación.

2.5.1 ANF Autoridad de Certificación.

La función de *ANF AC* es la emisión de los certificados digitales, y la administración y control de la infraestructura de certificación que se describe en esta *DPC*.

ANF AC para la prestación de sus servicios de certificación puede contar con la colaboración de Autoridades de Registro. En cualquiera caso, *ANF*

AC es la única entidad que decide sobre la aceptación o la denegación de una solicitud de certificado, su activación y publicación.

2.5.2 Autoridad de Registro Reconocidas.

Las Autoridades de Registro Reconocidas (*en adelante ARR*) son personas físicas o jurídicas nombradas por ANF AC , las cuales se comprometen a seguir las normas que al respecto se establecen en esta *DPC* y su addenda.

Las *ARR* son competentes para la tramitación de las solicitudes de certificados electrónicos ante ANF AC. Entre otras funciones, están capacitadas para determinar la adecuación de los peticionarios a los tipos de certificados que solicitan. Su responsabilidad principal es la de realizar labores de identificación y autentificación, tramitación, e información de las obligaciones y derechos que de los usuarios.

2.5.3 Entidades finales.

Usuarios - Suscriptores

Son todas aquellas personas físicas o jurídicas que son titulares, o que constan como representantes de los titulares de certificados emitidos por ANF AC .

Terceros de confianza

De forma general, son todas aquellas personas físicas o jurídicas que de forma voluntaria confían en los certificados emitidos por ANF AC .

2.5.4 Ámbito de aplicación.

Las Políticas de Certificación aplicadas por ANF AC y definidas en esta *DPC* determinan el uso apropiado que debe darse a cada tipo de certificado.

Cada Política de Certificación dispone de un identificador de objeto (OID) único, que además identifica el tipo y versión del documento.

En la sección “Certificados electrónicos” de este documento, se detallan los distintos tipos de certificados que se emiten, con sus respectivos identificadores OID.

2.6 Control de exportación.

La exportación de determinados elementos empleados por los servicios de certificación de ANF AC puede requerir la aprobación por parte del organismo público pertinente. Cuando esta normativa sea aplicable, los usuarios se ajustarán a las normas de control de exportación vigentes en cada momento.

2.7 Derechos de Propiedad Intelectual.

ANF AC es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que describe y regula este documento.

ANF AC posee todos los derechos de propiedad intelectual sobre esta *DPC*, sus ANEXOS, las Políticas de Certificación y en general el modelo de Sistema PKI.

Se autoriza su reproducción y difusión siempre que se reseñe:

-Copyright © ANF Autoridad de Certificación-

Los certificados, claves, y en general cualesquiera otros documentos, información o material de cualquier naturaleza que ANF AC ponga a disposición de los titulares de certificados, son propiedad intelectual de ANF AC . Se concede un permiso no exclusivo y no retribuido de reproducción y distribución de certificados a las partes, siempre y cuando se respete la integridad de los mismos y no se publiquen en un depósito público sin permiso de ANF AC.

Los nombres distintivos son propiedad de las personas que sustentan los derechos de marca correspondiente sobre los mismos, de existir. Si no se conoce esta circunstancia, ANF AC empleará el nombre propuesto por el usuario, bajo la entera responsabilidad de éste. Las claves privadas y públicas son propiedad de los usuarios, con independencia del medio físico empleado para almacenarlas y protegerlas.

Queda prohibido el uso total o parcial de cualquiera de los *OID* asignados a ANF AC salvo para el desarrollo de la actividad específica para los que se incluyeron en este documento, en las Políticas de Certificación, Anexos, o en los certificados emitidos por ANF AC.

3. Información General.

Esta *DPC* de ANF AC constituye una declaración de los criterios que se compromete a seguir este Prestador de Servicios de Certificación (*en adelante PSC*).

En esta *DPC* se exponen las normas y condiciones generales de los servicios de certificación que presta ANF AC , incluyendo la solicitud, identificación, generación, activación, revocación de los certificados, así como gestión y uso de los dispositivos de generación de firma y verificación. Es parte integrante de este documento sus Anexos y las Políticas de Certificación a la que se somete cada uno de los distintos tipos de certificados que ANF AC emite.

Esta versión 2 contempla las medidas adoptadas por este *PSC* tras haber pasado el algoritmo SHA-1 a situación de riesgo, y haber sido publicada la Política de Firma Electrónica, OID 1.3.6.1.4.1.18332.27. Así como la emisión de un nuevo certificado raíz ANF Server CA número de serie 01 34 4b.

Este documento está dirigido a todos los suscriptores de ANF AC y, en especial, a los terceros de confianza de este sistema abierto de certificación electrónica, personas que reciben ficheros electrónicos firmados digitalmente por los usuarios de ANF AC .

Caso de que el lector no conozca los conceptos básicos de un Sistema Abierto de Certificación Electrónica, ANF AC pone a su disposición un servicio gratuito de Atención al Cliente, y recomienda solicitar esta asistencia antes de continuar con la lectura de este documento.

3.1 El propósito.

De forma general cabe citar que las Políticas de Certificación declaran “lo que será adherido”, mientras que la Declaración de Prácticas de Certificación declara “como se adhiere”, es decir, que procesos realiza para generar y emitir los certificados electrónicos.

Estos documentos están disponibles al público de forma gratuita. La difusión de este documento está limitada con las restricciones indicadas en el apartado "*Derechos de Propiedad Intelectual".*

3.2 Documentación.

Este documento describe solo las reglas generales que ANF AC se compromete a seguir en la prestación de sus servicios de certificación. La descripción detallada del sistema se describe en documentos adicionales, parte de ellos solo son accesibles a personal autorizado.

La relación de documentos que emplea la organización se detalla en la Tabla 1.

Tabla 1

Nº	Nombre del Documento	Estado	Localización
1	Declaración de Prácticas de Certificación	Público	https://www.anf.es/AC/documentos/
2	Políticas vinculadas	Públicos	https://www.anf.es/AC/documentos/
3	Código ético de protección de datos personales	Público	https://www.anf.es/AC/documentos/
4	Seguridad Administrativa	Público	https://www.anf.es/AC/documentos/
5	Normas y criterios de auditoria de los Servicios de Certificación	Públicos	https://www.anf.es/AC/documentos/
6	Procedimientos de utilización de los componentes criptográficos.	Públicos	https://www.anf.es/AC/documentos/
7	Documentación técnica de la Base de Datos	No-público	Acceso restringido a personal autorizado
8	Procedimiento de la TSA para el archivo y destrucción de claves.	No-público	Acceso restringido a personal autorizado
9	Documentación técnica del sistema de detección de intrusos.	No-público	Acceso restringido a personal autorizado
10	Documentación técnica del sistema de supervisión permanente de servidores.	No-público	Acceso restringido a personal autorizado
11	Documentación técnica del hardware Servidores.	No-público	Acceso restringido a personal autorizado
12	Documentación técnica del diseño de los TSU	No-público	Acceso restringido a personal autorizado

13	Documentación procedimientos TSS	No-público	Acceso restringido a personal autorizado
14	Documentación técnica del diseño del servicio OCSP	No-público	Acceso restringido a personal autorizado
15	Documentación técnica de los procedimientos de copia y restauración.	No-público	Acceso restringido a personal autorizado
16	Documentación técnica del diseño de los dispositivos ARR.	No-público	Acceso restringido a personal autorizado
17	Documentación técnica del diseño de los servicios de notariado y factura delegada.	No-público	Acceso restringido a personal autorizado
18	Documentación técnica del diseño de los dispositivos entidad final.	No-público	Acceso restringido a personal autorizado
19	Documentación técnica del sistema de emisión certificados.	No-público	Acceso restringido a personal autorizado
20	Documentación técnica de los protocolos de comunicaciones.	No-público	Acceso restringido a personal autorizado
21	Normas en la asignación de puertos y reglas de filtrado.	No-público	Acceso restringido a personal autorizado
22	Plan de Contingencias y Seguridad de la Información.	No-público	Acceso restringido a personal autorizado
23	Análisis de Riesgos.	No-público	Acceso restringido a personal autorizado
24	Plan de Recuperación en caso de Desastre	No-público	Acceso restringido a personal autorizado
25	Plan de Continuidad del Negocio	No-público	Acceso restringido a personal autorizado
26	Procedimiento regulador de visitas al Centro de Procesamiento de Datos.	No-público	Acceso restringido a personal autorizado
27	Procedimiento y normas de trabajo del departamento de criptoanálisis.	No-público	Acceso restringido a personal autorizado

4. Definiciones y abreviaturas.

Además de las definiciones reseñadas en el anterior apartado, en la redacción de este documento se emplean:

Glosario de términos.

Contenedor	Soporte homologado por *ANF AC*, que contiene los datos de creación de firma.
Criptosistema asimétrico	Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar esa firma digital.
Entidad final	Persona, física o jurídica, titular de un certificado digital que no puede emitir otros certificados, es decir, que no es un PSC.
ETSI	Contracción del vocablo inglés "European Telecomunications Standards Institute", Instituto Europeo de Normas de Telecomunicaciones.
ITU	"International Telecommunication Union". Unión Internacional de Telecomunicaciones.
ITSEC	"Information Technology Security Evaluation Criteria".
PIN	Contraseña secreta que precisa el Contenedor para poder ser activado.
PKCS#7	"Crytographic Message Syntax Standard". Define una sintaxis para mensajes que incluyen procesos criptográficos, como firma electrónica y/o cifrado.
PKCS#10	"Certification Request Syntax Standard". Define la sintaxis de una petición de certificado.
PKCS#15	Es uno de los contenedores homologados de *ANF AC* . Sigue el estándar RSA http://www.rsasecurity.com/rsalabs/pkcs/pkcs-15/index.html
RFC	Contracción del vocablo inglés "Request For Comments". Documentos que se iniciaron en 1967 que describen los protocolos de Internet.
Receptor	Tercero de confianza; persona física o jurídica que recibe un fichero electrónico firmado digitalmente por un usuario de *ANF AC* . Los requisitos de la buena fe de los receptores se determinan en el presente documento.
Plug & Sign	Conjunto de programas e instrumentos homologados por *ANF AC*. Este sistema asume todo el proceso necesario para la generación de claves, creación y verificación de firma electrónica. En servicios telemáticos, asume la seguridad de las comunicaciones, procesos de identificación y autenticación.

Subject	Es el titular de un certificado emitido por *ANF AC* . (*en sistemas operativos que trabajan en lengua española aparece bajo la denominación "Asunto"*)
Suscriptor	Entidad que suscribe un certificado con un PSC en nombre de uno o más sujetos (personas físicas o jurídicas).
Usuario	Titular de un certificado emitido por *ANF AC*.
X-501	Estándar desarrollado por la UIT define las recomendaciones del Directorio. Incluido en el RFC 3039
X-509	Estándar desarrollado por la UIT para las PKI y los certificados de atributos. Incluido en el RFC 3281 – RFC 4476

Abreviaturas y acrónimos.

AC	Autoridad de Certificación = CA
ARR	Autoridad de Registro Reconocida
C	Contracción del vocablo inglés "Country", en español "País".
CEN	Contracción del vocablo inglés "Comité Européen de Normalisation".
CN	Contracción del vocablo inglés "Common Name", en español "Nombre Común. Componente Nombre. Es un atributo que forma parte del DN.
CPS	"Certificate Practice Statement" - Declaración de Prácticas de Certificación "DPC".
CRL	Contracción del vocablo inglés "Certificate Revocation List" . Lista de Revocación de Certificados suspendidos o revocados, en ella no constan los caducados.
CWA	Contracción del vocablo inglés "Cen Workshop Agreements."
DN	Contracción del vocablo inglés "Distinguished Name". En español "Nombre Distintivo". Conjunto de valores que identifican al certificado.
DPC	"Declaración de Prácticas de Certificación" - Certificate Practice Statement "CPS".
FTP	Protocolo de transferencia de registros "File Transfer Protocol"
GMT	Hora del meridiano de Greenwich "Greenwich Mean Time"
HTTP	Protocolo de transferencia de hipertexto "Hypertext Transfer Protocol"
IEC	Contracción del vocablo inglés "Information Evaluation Criteria".
ISO	Organización Internacional de Normalización.
ITSEC	"Information Technology Security Evaluation Criteria".
NTP	Contracción del vocablo inglés "Network Time Protocol"
O	Contracción del vocablo inglés "Organization". En español "Organización"
OCSP	Contracción del vocablo inglés "Online Certificate Status Protocol" – Protocolo informático que permite determinar la vigencia de un certificado electrónico.
OU	Contracción del vocablo inglés "OrganizationalUnitName". En español "Unidad Organizativa"
PIN	Número de Identificación Personal. Es la contracción de "Personal Identification Number"
PKCS	Estándares de criptografía de Clave Pública "Public Key Cryptography Standards"

SSCD	“Secure Signature –creation Device” Dispositivo Seguro de Creación de Firma.
UIT	Unión Internacional de Telecomunicaciones, organización internacional de las Naciones Unidas para coordinación de servicios de redes de telecomunicaciones entre Gobiernos y empresas.
URL	Localizador de recursos uniforme “Uniform Resource Locator”
UTC	Contracción del vocablo inglés “Universal Time Coordinated”.
WWW	Contracción del vocablo inglés “Word Wide Web”.

5. Documento de Seguridad.

La Declaración de Practicas de Certificación del *PSC*, tiene la consideración de Documento de Seguridad a los efectos previstos en normas relativas a la Protección de Datos de Carácter Personal.

El presente apartado recoge las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados en la Protección de Datos de Carácter Personal.

Este Documento de Seguridad es de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de ANF AC , incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deben ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

ANF AC para el desarrollo de su actividad como *PSC*, precisa disponer de datos personales de los solicitantes de certificados, además es necesario para la adecuada prestación del servicio en una PKI pública, facilitar el acceso público a la información contenida en los certificados y determinar su estado de vigencia.

Los ficheros sujetos a las medidas de seguridad establecidas en este documento, con nivel de seguridad básico, son los siguientes:

Nombre del fichero : **CLIENTES**

Descripción : DATOS SOBRE DENOMINACION, DOMICILIO, D.N.I., FORMA DE PAGO Y PARA PRESTACION DE SERVICIOS DE FIRMA ELECTRONICA.

Finalidad : GESTION DE LA RELACION COMERCIAL EN TODAS SUS VERTIENTES Y SERVICIOS DE FIRMA ELECTRONICA

Nombre del fichero : **USUARIOS**

Descripción : DATOS PERSONALES DE SUSCRIPTORES DE CERTIFICADOS DIGITALES.

Finalidad : GESTION Y MANTENIMIENTO DE LAS PERSONAS QUE HAN SOLICITADO CERTIFICADOS DIGITALES

Nombre del fichero : **CERTIFICADOS ELECTRÓNICOS**

Descripción : INFORMACION DE LOS CERTIFICADOS ELECTRONICOS EXPEDIDOS POR LA EMPRESA.

Finalidad : GESTION DE LA EMISION, ADMINISTRACION Y CONSULTA PUBLICA DE LOS CERTIFICADOS POR EMITIDOS POR LA EMPRESA.

Nombre del fichero : **COLABORADORES EXTERNOS**

Descripción : FICHEROS DE DATOS PERSONALES DE COLABORADORES EXTERNOS DE LA EMPRESA.

Finalidad : GESTION Y CONTROL DE RELACIONES PROFESIONALES CON LOS COLABORADORES EXTERNOS DE LA EMPRESA.

Nombre del fichero : **PROVEEDORES**

Descripción : FICHERO DE PROVEEDORES DE LA EMPRESA.

Finalidad : GESTION, CUMPLIMIENTO Y CONTROL DE LAS RELACIONES COMERCIALES CON LOS PROVEEDORES DE LA EMPRESA.

Nombre del fichero : **RECURSOS HUMANOS**

Descripción : FICHERO DE DATOS DE PERSONAL DE LA EMPRESA.

Finalidad : GESTION DE LOS RECURSOS HUMANOS DE LA EMPRESA

Nombre del fichero : **CONTRASEÑAS**

Descripción : FICHERO DE DATOS DE CONTRASEÑAS DE ACCESO A LOS SERVICIOS TELEMÁTICOS, ASÍ COMO PREGUNTAS Y RESPUESTAS.

Finalidad : GESTION DEL CONTROL DE ACCESOS Y PROCEDIMIENTO PARA MODIFICAR UNA CONTRASEÑA EN CASO DE OLVIDO.

Esta *DPC* y su addenda, es de obligado cumplimiento para el personal con acceso a los datos personales y a los sistemas de tratamiento de la información.

ANF AC, es el *Responsable del Fichero*, actúa como *Responsable de Seguridad* el *Responsable de Seguridad* del área jurídica, asumiendo, formalmente, la función de coordinar y controlar las medidas de seguridad aplicables.

ANF AC, informa a todos los Usuarios de estos servicios de su derecho de información, oposición, acceso, rectificación y cancelación de los datos. Este derecho se extiende a las personas físicas a las que representan los Usuarios. Puede ser ejercitado enviando un correo electrónico a:

ac@anf.es

Personalmente o por correo dirigido a:

ANF AC
Gran Vía de les Corts Catalanes, 996 – 4
08020 – Barcelona - España

Las incidencias relacionadas con los datos de carácter personal, son resueltas por personal del departamento jurídico, y siguiendo el procedimiento descrito en el apartado "Procedimiento de reclamación" de este documento. Además *ANF AC* sigue el siguiente protocolo en el tratamiento de toda incidencia:

- Se registra el tipo de incidencia.
- Momento en que se ha producido.
- Persona que la notifica.
- Persona a la que se comunica.
- Efectos derivados.

Previo al inicio del trámite, el requirente debe de identificarse ante ANF AC. Para ello puede optar por cualquiera de los medios que al efecto tiene incorporados este *PSC,* en su *DPC* y *Políticas de Certificación.*

ANF AC en el desarrollo de sus normas de seguridad, ha tomado como guía las orientaciones y recomendaciones especificadas en la versión ISO/IEC 17799:2005. Apartados:

- Política de seguridad: proporcionar directivas y consejos de gestión para mejorar la seguridad de los datos.

- Seguridad de la organización: facilitar la gestión de la seguridad de la información en el seno de la organización.

- Clasificación y control de los activos: catalogar los activos y protegerlos eficazmente.

- Seguridad del personal: reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos.

- Seguridad física y medioambiental: impedir la violación, el deterioro y la perturbación de las instalaciones y datos industriales.

- Gestión de las comunicaciones y operaciones: garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información.

- Control de accesos: controlar el acceso a los datos.

- Adquisición, Desarrollo y mantenimiento de los sistemas: garantizar que la seguridad esté incorporada a los sistemas de información.

- Gestión de incidentes de seguridad de la información

- Gestión de la continuidad de las operaciones de la empresa: reducir los efectos de las interrupciones de actividad y proteger los procesos esenciales de la empresa contra las averías y los siniestros mayores.

- Conformidad: prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales y las exigencias de seguridad.

La seguridad desarrollada por *ANF AC* tiene como ejes principales de actuación:

- Los servicios de seguridad requeridos para satisfacer las necesidades de sus usuarios.

- Los servicios de seguridad requeridos para la protección de las claves privadas, y el código fuente del software empleado por los usuarios y el propio *PSC*.

- Los servicios de seguridad requeridos para que el sistema atienda las obligaciones que le impone la legislación vigente.

- Los servicios de seguridad requeridos para que el sistema proporcione protección ante ataques conocidos sobre sistemas de certificación y firma electrónica.

- Los elementos del sistema requeridos para implementar esos servicios.

- Los niveles de desempeño que se requiere de los elementos para que interactúen con las amenazas del entorno.

- La arquitectura de seguridad considera tanto amenazas de tipo intencional e inteligente, como de tipo accidental.

Este documento se ha desarrollado, en coherencia con las Directivas y normas legales cuyo detalle consta en el apartado "Normas y estándares" de esta *DPC*.

La documentación que especifica los procedimientos de alta seguridad implantados en la PKI de ANF AC, está clasificada con carácter confidencial y es por tanto de acceso restringido, Seguidamente se informa de aquellos aspectos que, estimando pueden ser de interés de los usuarios de este *PSC* y preceptivos por la legislación vigente, no quebrantan la necesaria privacidad que tiene que prevalecer en esta materia.

5.1 Seguridad Administrativa.

La Seguridad Administrativa en ANF AC está regulada por un Plan de Seguridad. Este Plan establece medidas técnicas y organizativas.

El detalle del Plan de Seguridad Administrativa queda reseñado en el ANEXO II.

5.2 Seguridad de los equipos informáticos.

El sistema informático de ANF AC, dispone de un procedimiento de detección y registro de intentos de accesos no autorizados. Se registra:

- Procedencia del operador.
- Día y hora del ataque.
- Zonas que se han intentado acceder.
- Manipulaciones que se han efectuado.

Todos los equipos informáticos, en especial aquellos que son utilizados para el tratamiento de datos personales, están inventariados e identificados con el nivel de acceso que tienen a los datos de carácter personal almacenados, y el grado de importancia que presuponen en el marco del tratamiento de la información que realiza este *PSC*.

Cualquier salida o incorporación de equipos utilizados en el tratamiento de la información, debe de ser autorizada por el Responsable del área de Informática, el cual es además, responsable del mantenimiento del inventario de equipos, su catálogo de uso y en especial, en aquellos dispositivos que almacenan información, la identificación del tipo de datos que contienen.

5.2.a Fluido eléctrico.

Todos los servidores que prestan servicio al público, están conectados a un estabilizador de corriente que impide que los ordenadores sufran variaciones eléctricas.

En caso de cortes eléctricos por parte de la compañía suministradora, el fluido eléctrico permanece gracias a un sistema de acumuladores que garantizan el servicio durante 3 horas; transcurrido ese periodo, y si el corte eléctrico permanece, el servicio queda asegurado mediante generadores eléctricos que se encuentran permanentemente en las instalaciones donde se ubican los equipos informáticos.

5.2.b Comunicaciones.

El ancho de banda a la Red (Internet), es contratado directamente a las primeras operadoras de comunicaciones, especificando en los correspondientes contratos los deberes y las garantías exigidas sobre medidas de seguridad en los tratamientos, confidencialidad y secreto de las comunicaciones.

La accesibilidad de los usuarios al sistema de ANF AC está garantizado mediante un sistema de equipos informáticos que trabajan en espejo; si la dirección principal Web queda fuera de servicio, las necesidades esenciales de los usuarios pueden continuar siendo atendidas: Revocación, verificación del estado de los certificados emitidos, firma electrónica y sellos de tiempo.

El sistema está dotado de un mecanismo de protección adicional de los sistemas de ANF AC, implementando dispositivos de protección "firewalls".

Los sistemas y dispositivos de protección ("firewalls") han sido configurados de conformidad con las políticas de seguridad de entidades especialistas en la materia y de reconocido prestigio.

ANF AC retiene los datos de tráfico relativos a las comunicaciones electrónicas que se realizan con sus servidores de Internet. Concretamente:

Retiene los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses.
Los datos retenidos son únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información: número de IP, día y hora de acceso, puerto de acceso, operaciones realizadas y servicio al que se ha accedido. En ningún caso, la obligación de retención de datos afecta al secreto de las comunicaciones.

ANF AC adopta medidas de seguridad apropiadas para evitar la pérdida o alteración y el acceso no autorizado a los datos de tráfico retenidos. Estos datos tienen como único fin y destino:

Para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales.

Categoría de los datos retenidos:

Básica:

- Servicio de acceso a los repositorios de certificados emitidos.
- Servicio de acceso a los repositorios de certificados revocados.
- Área privada.

Crítica

Servicio de revocación de certificados.
Servicio de reactivación de certificados.
Servicio de renovación de certificados.
Servicio de recepción de certificados de petición.
Servicio de Sellos de Tiempo.

En todos los casos, los datos son almacenados en un soporte magnético que se encuentra en lugar custodiado y de acceso restringido. Este soporte esta etiquetado con un identificador único, inventariado, precintado y firmado por el responsable de seguridad.
Transcurrido el plazo de retención previsto, los datos se destruirán salvo que fueran necesarios para otros fines previstos por la Ley. El proceso de destrucción de los datos seguirá el siguiente procedimiento:

Borrado de la información.
Escritura en disco.
Borrado de la información.
Formateo del dispositivo a bajo nivel.

El plazo de retención será de:

6 meses para la categoría básica.
12 meses para la categoría crítica.

Los datos serán entregados a los órganos autorizados en soporte óptico.

5.2.c Hardware.

5.2.c.a Equipo Informático

Todo el material informático utilizado para dar servicio en la red es estándar. ANF AC cuenta con ordenadores y copias de seguridad, para poder proceder a una sustitución prácticamente inmediata en caso de producirse un fallo en los equipos de atención al público.

La arquitectura del sistema, está formada por una "intranet". Una parte de los ordenadores está conectada a Internet; estos equipos son los que dan servicio Web. El resto de los equipos, no tienen conexión a Internet y sólo atienden operaciones llevadas a cabo en la propia "intranet"; estos ordenadores están destinados a asumir distintas operaciones: copias de seguridad, servicio base de datos, almacén de certificados, códigos fuente de software...etc. Además de lo reseñado, ANF AC cuenta con equipos informáticos sin conexión a Internet ni a la propia Intranet, estos equipos se destinan a funciones especificas como: emisión de certificados y desarrollo de software.

Cada uno de los ordenadores empleados: servidores y estaciones de trabajo, son de uso exclusivo de ANF AC. En ningún caso se realiza en ellos hospedaje de terceros ni suministro de cuentas de acceso.

Todos los ordenadores controlan el acceso de los operadores mediante sus certificados digitales personales.

Todo el personal de ANF AC está dotado de certificados digitales que lo identifican y determinan el nivel de accesibilidad que poseen.

5.2.c.b Dispositivos criptográficos

Parte de los servidores de *ANF AC* tienen instalados dispositivos criptográficos, sobre estos dispositivos se establecen los siguientes requerimientos:

- 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.
- 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.
- 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.
- 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. Se procede a efectuar la correspondiente anotación en el inventario de la entidad.
- Se exige a los proveedores del hardware criptográfico que procedan a su transporte utilizando un embalaje inviolable. La recepción de este material es encomendada a personal autorizado de *ANF AC*, el cual revisa que el embalaje y los precintos se encuentren intactos, seguidamente se efectúa un test de aceptación y verificación de los soportes lógicos
- 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 .

- 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.

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:

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 *PSC* 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 auditoria y procedimientos para verificar la efectividad de los controles.

El hardware criptográfico de ANF AC es almacenado en embalajes inviolables.

El manejo del hardware criptográfico de ANF AC se efectúa en presencia de no menos de dos empleados confiables.

La instalación del hardware criptográfico de ANF AC se efectúa en presencia de no menos de dos empleados confiables.

La eliminación del hardware criptográfico de ANF AC de producción, se efectúa en presencia de no menos de dos empleados confiables.

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.

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.

5.2.d Software.

Este *PSC* sólo utiliza software original y de licencia autorizada, y se responsabiliza de mantener su sistema operativo actualizado.

Los equipos de ANF AC tienen instalado un sistema de sincronización horaria.

5.2.e Copias de seguridad.

Diariamente se realizan copias de seguridad del sistema. Se mantiene una copia del día, de la semana, del mes y un histórico semestral.

El personal encargado de su realización queda reseñado en el ANEXO II

El protocolo de copias de seguridad establecido mantiene una copia diaria de los últimos 7 días, una copia individual de cada una de las últimas 4 semanas, y permanente de cada una de las copias semestrales que se han realizado. Cada dispositivo de copia empleado es identificado con un código único mediante etiqueta de seguridad firmada y sellada.

Las copias quedan depositadas en la Caja de Seguridad Estanco y contraincendio en el DataCenter de ANF AC, estando inventariadas y debidamente codificadas a fin de determinar su contenido.

El almacenamiento a largo plazo de los registros se realiza en medios WORM ("escribir una vez leer muchas").

Copia del software de restauración de las copias de seguridad es integrada en cada uno de los soportes.

Semestralmente, con autorización del Responsable del Fichero, se realizan pruebas de las copias de seguridad efectuadas, al objeto de asegurar que éstas se han realizado correctamente y que en el caso de tener que recurrir a ellas, la recuperación podrá llevarse a cabo. El procedimiento seguido es:

Las pruebas se realizan seleccionando tres de los dispositivos que contienen copias diarias, semanales y mensuales. La copia semestral se verifica en el momento de su realización.

Para la comprobación del estado de las copias se realizan ficheros temporales, los cuales son borrados una vez finalizada la comprobación.

Son responsables de la verificación de las copias, el personal encargado de su realización, salvo la semestral que se realiza en presencia de dos responsables de *ANF AC*.

Se mantiene un inventario de los dispositivos y soportes de copia empleados por ANF AC. Este inventario detalla el lugar donde es almacenado, el contenido y la fecha de la copia. Los empleados responsables del sistema de copias de seguridad se responsabilizan del cumplimiento del sistema.

Se establece un periodo de vida de los soportes magnéticos de 24 meses, transcurrido ese periodo el soporte será desechado siguiendo el procedimiento establecido en el ANEXO II.

El método de recuperación de datos queda especificado en el ANEXO II

5.2.f Controles de seguridad informática.

ANF AC y sus *ARR* utilizan sistemas de confianza para desarrollar sus respectivas funciones, de conformidad con la presente *DPC*, Políticas de Certificación y Anexos. Entre los componentes de los controles de seguridad informática se cuentan:

- Cuentas de usuario individual para cada persona que integra el sistema operativo y el nivel de la administración de las solicitudes.
- El mantenimiento de los servicios básicos en los "host's" del sistema para permitir la prestación de servicios en conformidad con las presentes *DPC*.
- La realización periódica de un monitoreo de seguridad y de auditorias de las cuentas de usuario y de los "host's".
- La comprobación periódica de recursos disponibles y valoración de nuevas necesidades.

5.2.f .1 Tipos de eventos registrados.

ANF AC registra todos los eventos relacionados con:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo.
- Arranque y parada de aplicaciones.
- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar claves y certificados.
- Intentos exitosos o fracasados de generar, firmar o emitir una *CRL*.
- Intentos exitosos o fracasados de crear, modificar o borrar información de los titulares de certificados.

- Intentos exitosos o fracasados de acceso a las instalaciones por parte de personal autorizado
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal

5.2.f .2 Frecuencia de procesado de logs

Se establecen tres niveles de auditorías de control de los eventos registros con una frecuencia diaria, mensual y anual respectivamente.

5.2.f .3 Periodo de retención para los logs de auditoría

ANF AC retiene todos los registros de auditoría generados por el sistema por un periodo mínimo desde la fecha de su creación de un (1) años para los pertenecientes a auditorías diarias, dos (2) años para las mensuales y cuatro (4) años para los de auditorias anuales.

5.2.f .4 Protección de los logs de auditoría

Cada histórico de auditoría que contenga esos registros queda cifrada. Las copias de backup de dichos registros se almacena en un dispositivo dentro de las instalaciones seguras de la CA..

5.2.f .5 Procedimientos de backup de los logs de auditoría

Se realizará copia de los mismos sobre soporte óptico, grabando además en el mismo soporte el software necesario para poder proceder a su recuperación o consulta.

5.2.f .6 Sistema de recogida de información de auditoría (interno - externo)

El sistema de recolección de auditorías de la PKI es una combinación de procesos automáticos y manuales ejecutados por los sistemas operativos, la aplicación de la PKI, y por el personal que las utiliza.

5.2.f .7 Notificación al sujeto causa del evento

El administrador del sistema determinará en base a la gravedad del incidente detectado, si notifica el suceso a la persona que lo provocó. En caso de tratarse de una evento calificado como grave, será notificado directamente a la Junta Rectora de la PKI.

5.3 Seguridad del personal.

El Plan de Seguridad incluye un documento de obligado cumplimiento para el personal con acceso a los ficheros y a los sistemas de información. Se establece la forma de integración de la normativa y una actividad dedicada a la formación de los responsables de los ficheros y de seguridad.

El Responsable de Seguridad mantiene una relación actualizada de los usuarios y accesos autorizados.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con siguiente procedimiento:

- Formación.
- Puesta disposición permanente de la documentación correspondiente.
- Puesta a su disposición permanente, de personal que atienda sus consultas.
- Firma, por parte del personal, confirmando haber leído y saber interpretar las normas y consecuencias por incumplimiento.

5.3.1 Requisitos.

5.3.1.a Formación

Todo el personal empleado por este *PSC* con acceso al sistema, cuenta con la formación adecuada para la función que tiene encomendada de acuerdo con las áreas donde realiza su labor. Están establecidos los siguientes criterios:

a) **Área informática y telecomunicaciones**: Ingeniero técnico en telecomunicaciones o informática.
b) **Área jurídica**: Licenciado en Derecho.
c) **Área de administrativa**: Especialista en Protección de Datos y Seguridad Informática.
d) **Área comercial**: Especialista en Protección de Datos y Seguridad Informática.

Todo el personal empleado por *ANF AC* tiene acceso permanente a la Declaración de Prácticas de Certificación, Políticas de Certificación, Anexos y Política de Privacidad. El personal técnico puede pertenecer a la infraestructura de recursos humanos de la matriz *ANF AC.*

5.3.1.b Selección, conocimientos y experiencia.

La selección del personal se efectúa siguiendo los siguientes parámetros:

1/ Estar en posesión del titulo o licenciatura de acuerdo al área donde va a realizar su actividad.
2/ Contar con formación adecuada a la materia especifica que va a desarrollar. Se verifica el nivel de conocimientos realizando un test que permita comprobar las exigencias básicas establecidas.
3/ Se efectúan comprobaciones de las referencias y antecedentes laborales de los candidatos.
4/ Se exige una antigüedad mínima y ostentar determinados cargos en la compañía, para poder acceder a determinadas funciones de confiabilidad.
5/ Conocimientos y experiencia sobre entornos de certificación digital.

Son considerados puestos de confianza, aquellos que permite el acceso a los servicios de certificación de ANF AC .

Se han implementado procedimientos de evaluación y formación continúa del personal para verificar que las aptitudes, la experiencia y la

capacitación de cada individuo integrado en ANF AC sean las adecuadas para el cargo ejercido.

5.3.2 Identificación y autenticación para cada función.

Según lo especificado en la norma CEN CWA 14167-1, se han contemplado una serie de funciones básicas que constan detalladas en este apartado.

Toda persona que tiene funciones de confianza cuenta con autorización para realizarlas. La asignación de funciones de confianza a un empleado están adecuadamente documentadas.

Todo el personal es conocedor de la parte del Documento de Seguridad que le afecta en sus funciones, firmando el correspondiente documento acreditativo de dicha notificación.

El acceso a los datos está restringido a los usuarios autorizados conforme a los mecanismos y medidas definidas por el Responsable de Seguridad. El proceso de identificación y autentificación ante el sistema, es asumido mediante procedimientos de firma electrónica.

El *Responsable de Seguridad* dispone de una relación de usuarios con acceso autorizado, según perfil, a los sistemas de información.

La definición de los puestos de trabajo y sus responsabilidades, incluidas las de seguridad, se integran en el Convenio que regula las relaciones de trabajo entre el personal que las realiza y ANF AC .

Las funciones de confianza identificadas para el control y la gestión del sistema son:

a. Responsables de emisión de certificados.
b. Directores de área.
c. Administrador de Sistemas.
d. Operadores de la Autoridad de Certificación.
e. Responsable de selección y formación.

f. Responsable de Seguridad.
g. Auditor.
h. Responsable de la elaboración de Dictámenes de emisión y revocación de certificados.
i. Responsable de Documentación.

5.3.2.a Responsables de emisión de certificados.

Son un mínimo de cuatro los operadores, los que cuentan con la capacidad para acceder y activar los dispositivos de emisión de certificados de ANF AC .

Para activar las claves, es necesaria la presencia de al menos tres personas. Dos de ellas asumiendo la función de Responsable de emisión de certificados y un tercero perteneciente al equipo de seguridad del centro de datos (sin capacidad de acceso a las claves).

5.3.2.b Directores de Área.

Son las personas que asumen la dirección de cada sección de ANF AC. Bajo su control y supervisión, se encuentra el personal adscrito a la misma. Es su responsabilidad:

- Recibir y dan curso a las denuncias por infracciones que puedan afectar a su personal, proponiendo las medidas disciplinarias correspondientes.

- Efectuar un control permanente de la adecuación de los recursos materiales y humanos que cuenta su Departamento, con el fin de atender las necesidades de servicio que tiene encomendadas.

5.3.2.c Administrador de Sistemas.

Adscrito al área de Informática y Telecomunicaciones.
Ningún de ellos esta implicado en tareas de auditoría interna.

- Responsables de la instalación y configuración de sistemas operativos, de productos software, del mantenimiento y actualización de los productos y programas instalados. Con capacidad para configurar, mantener los sistemas, pero sin acceso a los datos.
- Responsables de activar los servicios de *CRL's*, *OCSP*, *Timestamping*, mediante certificados específicos.
- Encargados de establecer y documentar los procedimientos de monitorización de los sistemas y de los servicios que prestan, así como del control de las tareas realizadas por los Operadores de Autoridad de Certificación.
- Responsables del diseño de las arquitecturas de programación, del control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones.
- Responsables de supervisar la correcta ejecución de la Política de Copias y, en particular, y de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible. Velar para que se lleven a cabo las copias de backup locales y del traslado de las mismas de acuerdo con lo establecido en el Plan de Seguridad.
- Responsables de mantener el inventario de servidores y resto de componentes de los sistemas de certificación de ANF AC .
- Asumen la gestión de los servicios de "router" y gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusiones, etc.).

5.3.2.d Operadores de la Autoridad de Certificación.

Adscrito al área administrativa.

Labores administrativas que no requieren acceso físico a los Servidores de Certificación.

Efectúan labores administrativas tradicionales: archivo, introducción de datos, recepción y expedición de correo, atención de visitas y llamadas telefónicas, etc.

Esencialmente colaboran en todas aquellas funciones que le son requeridas por los directores de área, bajo cuyo criterio se organiza su trabajo y delegación de responsabilidades.

Deben de haber efectuado una formación específica en materia de protección de datos y seguridad informática, superando los test correspondientes. Se exige una experiencia mínima de un año en funciones administrativas.

5.3.2.e Responsable de selección y formación.

Adscrito al Área jurídica.

Responsable de selección y formación.

Se encarga de mantener actualizados los planes de formación del personal que presta sus servicios en ANF AC.

Supervisa la realización de la formación por parte del personal y lleva a cabo los test necesarios para poder evaluar el nivel adecuado de conocimientos asimilados.

Gestiona la selección de nuevo personal, controlando la obtención de referencias y del cumplimiento de los niveles establecidos.

Se exige una experiencia mínima de dos años en este tipo de funciones.

5.3.2.f Responsable de Seguridad.

Adscrito al área jurídica.

Asume la responsabilidad general en cuanto a la actualización e implantación de las políticas y procedimientos de seguridad que han sido aprobadas por la Junta Rectora de ANF AC.

Controla la formalización de los convenios entre el personal y ANF AC.

Comunica las medidas disciplinarias acordadas, supervisando su cumplimiento.

Debe cumplir y hacer cumplir las políticas de seguridad de ANF AC, y debe encargarse de cualquier aspecto relativo a la seguridad de la *PKI*, desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red.

Es el encargado de gestionar los sistemas de protección perimetral y en concreto de verificar la correcta gestión de las reglas de los firewalls.

Es el encargado de comprobar la correcta instalación, configuración y gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.

Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc.

Es el responsable de la gestión y control de los sistemas de seguridad física de la PKI.

Debe encargarse de efectuar la selección y determinar la contratación de terceros especialistas que puedan colaborar en la mejora de la seguridad de ANF AC .

Se exige una experiencia mínima de un año en funciones.

5.3.2.g Auditores.

Adscritos al área jurídica y, al área de Informática y Telecomunicaciones.

Auditoria interna.

Los auditores internos asumen la responsabilidad de:

> Realizar la Auditoria Interna de acuerdo con las Normas y Criterios de Auditoria de los Servicios de Certificación (ANF AC) OID 1.3.6.1.4.1.18332.11.1

Cuentan con la capacidad de acceder a los logs del sistema.

Se exige una pertenencia mínima de un año en el área relacionada.

5.3.2.h Responsable de la elaboración de Dictámenes de emisión y revocación de certificados.

Adscrito al Área jurídica

Asume las responsabilidades establecidas en esta *DPC*, para el desempeño de estas funciones. Especialmente asume la responsabilidad de aprobar o denegar la emisión de un certificado, o proceder a su revocación.

Se exige una pertenencia mínima de un año en el Área relacionada.

5.3.2.i Responsable de Documentación.

Adscrito al área administrativa.

Controla que el repositorio de documentación electrónica de ANF AC y los archivos de documentación en papel están actualizados.

Supervisa que se lleven a cabo las actualización de documentos cuando sea preciso.

Es el único habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación de ANF AC .

Se exige una pertenencia mínima de un año en el área relacionada.

5.3.3 Frecuencia y requisitos de capacitación.

ANF AC desarrolla ejercicios de capacitación cada vez que el personal que integra la AC necesite obtener un mayor grado de conocimiento sobre cualquiera de sus funciones. Anualmente, se llevan a cabo un mínimo de 20h. de formación en la materia que se considere necesaria para cubrir el adecuado desempeño de sus funciones y, en general, se realizará formación continua en materia de Seguridad Administrativa sobre los siguientes aspectos:

- Control de acceso.
- Gestión de soportes.
- Registro de Incidencias.
- Registro de Usuarios.
- Identificación y autenticación.
- Copias de respaldo y recuperación.
- Análisis de ficheros, datos y sistemas informáticos.
- Seguridad Administrativa. Plan de Seguridad.

5.3.4 Sanciones a las operaciones no autorizadas.

El personal esta sometido a un régimen disciplinario previamente advertido y conocido por todos los operarios de la organización. La operativa del procedimiento seguido queda documentada en el Anexo II de esta *DPC*.

La realización de operaciones no autorizadas esta sujeto a medidas disciplinarias, la sanción puede llegar al despido, con independencia de lo

establecido en el marco legislativo que puede conllevar paralelamente la denuncia ante la Autoridad Judicial.

5.3.5 Documentación entregada al personal.

Todo el personal de ANF AC recibe documentación vinculada con las descripciones, las funciones y las responsabilidades inherentes al cargo ocupado. Así mismo se detalla:

a) Necesidad de formación continua;
b) Los requerimientos contractuales que incluyen indemnizaciones por daños causados por acciones del personal contratado y,
c) El derecho de ANF AC a la auditoria y el monitoreo de la actividad desarrollada por el personal contratado.

5.3.6 Control de antecedentes del personal contratado.

El Departamento de Recursos Humanos de ANF AC lleva a cabo una verificación de los antecedentes de todo el personal. Como mínimo las comprobaciones a realizar alcanzan los siguientes aspectos:

- **Personal que desempeña roles confiables:**

Comprobación de antecedentes profesionales y obtención de referencias.
Comprobación de títulos y acreditaciones profesionales.
Verificación de datos de residencia.

- **Resto de personal**:
  - **a)** Comprobación de antecedentes profesionales y obtención de referencias.
  - **b)** Verificación de datos de residencia.

5.3.7 Acuerdo de confidencialidad.

Todo el personal con acceso a los servicios de certificación de *ANF AC* firma un acuerdo de confidencialidad como parte de los términos y condiciones de su incorporación. Este acuerdo contempla información sobre la labor de control y fiscalización que los responsables de seguridad

de ANF AC realizan permanentemente sobre el personal, el software y el hardware. El fin de esta actividad es garantizar el más alto grado de seguridad de los servicios que esta CA presta, y de los bienes que tiene la obligación de proteger.

La operativa del procedimiento seguido queda documentada en el Anexo II de esta *DPC.*

5.3.8 Procedimiento disciplinario.

Con el fin de cumplir la normativa interna de ANF AC y las obligaciones establecidas en la legislación vigente por la actividad desarrollada por esta entidad, ANF AC hace constar en los convenios suscritos con el personal colaborador que se reserva el derecho a inspeccionar de forma permanente o en cualquier momento, así como llevar un seguimiento de todos los sistemas que componen los servicios de certificación desarrollados por la entidad.

De forma enunciativa que no limitativa, los sistemas referenciados anteriormente comprenden:

> *Archivos de correo electrónico, soportes de almacenamiento internos o extraíbles de ordenadores personales, archivos de voz, colas de impresión, documentación fax, escritorios, así como sobres, cajas o bolsas que se encuentren en las instalaciones de* ANF AC .

5.3.9 Actividades no permitidas.

Salvo autorización expresa, no esta permitido instalar, utilizar o solicitar información de instrumentos que puedan ser empleados para evaluar o comprometer la seguridad de los sistemas de certificación de ANF AC. Tampoco se permite la instalación o utilización, sin autorización expresa, de instrumentos que tengan como fin cualquier intento de evaluación de los servicios que utiliza o recibe ANF AC.

Esta prohibición se extiende a cualquier intento de comprobación o intento de comprometer las medidas de seguridad de ANF AC, aunque no utilice instrumento alguno. En igual medida a la evaluación no autorizada de los servicios prestados o recibidos de ANF AC, se empleen o no dispositivos al efecto.

También esta expresamente prohibido la utilización de software o hardware que no este expresamente autorizado por la empresa, así como la instalación, almacenaje o distribución por cualquier medio

Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá activar los mecanismos de cambio de contraseña.

El usuario está obligado a utilizar los datos, la red corporativa y/o la intranet de la Entidad y/o de terceros sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la empresa y/o de terceros o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.

Compartir o facilitar el identificador de usuario y la clave de acceso facilitado por la Entidad a otra persona física o jurídica. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada su identificación de usuario.

Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Entidad.

Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones (revelación de secretos).

Intentar distorsionar o falsear los registros log del sistema.

Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la Entidad y/o de terceros.

Intentar aumentar el nivel de privilegios de un usuario en el sistema.

Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la Entidad o de terceros. (Estos actos pueden constituir un delito de daños.

El usuario no deberá almacenar datos de carácter personal en el disco duro del ordenador, sino utilizar para tal fin las carpetas de la red corporativa preasignada.

Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la organización, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario.

Introducir voluntariamente programas, virus, macros, applets, componentes ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los Sistemas Informáticos de la empresa o de terceros. Al respecto, recordar que el propio sistema ejecuta automáticamente los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.

Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la empresa; esta prohibición incluye cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.

Instalar copias ilegales de cualquier programa, incluidos los que están estandarizados.

Borrar cualquiera de los programas instalados legalmente.

Enviar o reenviar mensajes en cadena o de tipo piramidal.

Utilizar los recursos telemáticos de la empresa, incluida la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.

Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la empresa.

Cifrar información sin estar expresamente autorizado para ello.

5.3.10 Denuncia obligatoria.

Todos las posibles supuestos de infracción de la normativa del que tenga conocimiento o sospecha el personal de ANF AC , tiene la obligación de ponerlo en conocimiento de su Director de Área, o si la gravedad del caso lo requiriera, de la Dirección General de la entidad.

5.4 Seguridad física.

ANF AC garantiza que cumple la normativa aplicable en todos los aspectos de seguridad física y las describe en el presente apartado.

Se han establecido diferentes perímetros de seguridad con barreras de seguridad y controles de entrada adecuados a las actividades que se desarrollan en cada uno de ellos. Todo ello con el fin de reducir el riesgo de accesos no autorizados o de daños a los recursos informáticos.

5.4.1 Centro de Datos

Los equipos informáticos que prestan servicio público (principal y espejos) están instalados en Centros de Datos pertenecientes a primeras compañías nacionales, con las cuales rige el correspondiente contrato o convenio.

El edificio donde se encuentra instalada la infraestructura central de *ANF AC* es un recinto físicamente seguro, dotado de varios niveles de seguridad para poder llegar a acceder a las máquinas y aplicaciones críticas.

Entre las medidas de protección que poseen estas instalaciones, reseñar que:

Las instalaciones cuentan con servicio de vigilancia permanente.

Situación alejada de sótanos para prevenir posibles inundaciones.

La arquitectura del edificio corresponden al diseño comúnmente empleado en establecimientos denominados “Data center”.

El edificio es un inmueble moderno, construido al efecto y de uso exclusivo del operador. Ubicado en zona empresarial de reconocida, de fácil y rápido acceso, en caso de necesidad, por parte de los servicios de Orden Público y Bomberos.

El edificio se encuentra ubicado en zona de baja actividad sísmica y sin antecedentes de catástrofes naturales.

El edificio se encuentra ubicado en zona de bajos niveles de delincuencia.

Ni el edificio, ni la zona en donde se encuentra, están considerados objetivos terroristas.

La sala del Centro de Dato alojan los servidores, no tiene ventanas al exterior del edificio.

Las instalaciones se encuentran protegidas constantemente por personal de seguridad. Este personal tiene relación detallada y actualizada de las personas que ANF AC autoriza a acceder al núcleo central donde se encuentran los equipos informáticos, confeccionan un registro del día y hora de entrada y salida, identidad y firma de la persona que accede y de cada una de las personas que la acompañan, entregando tarjeta de acceso personal. En ningún caso permite la extracción de ordenadores sin autorización expresa.

El acceso al núcleo central se realiza superando distintos controles. El personal que accede se encuentra en todo momento acompañado por personal responsable de la administración del centro de datos y cualquier labor que se realiza sobre los equipos informáticos de ANF AC se realiza en presencia constante de un técnico perteneciente al personal responsable de la administración del centro de datos.

Todas las instalaciones cuentan con sistemas de energía y aire acondicionado, que cumplen con las normas industriales, a fin de crear un entorno operativo adecuado.

Todas las instalaciones cuentan con mecanismos de prevención destinados a reducir el efecto del contacto con el agua.

Todas las instalaciones cuentan con mecanismos de prevención y protección contra incendios. Dichos mecanismos cumplen con las normas industriales.

Todo el cableado esta protegido contra daños o interceptación electromagnética o interceptación de la transmisión tanto de datos como de telefonía.

Las mamparas que protegen las zonas centrales del núcleo son transparentes y cuentan con iluminación permanente, todo ello con el fin de

posibilitar la observación desde cámaras de vigilancia o desde pasillos o incluso zona de oficinas administrativas, impidiendo así actividades ilícitas en el interior.

5.4.1.a Acceso físico

Perímetro de seguridad física

Además de las medidas reseñadas anteriormente, se han implementado sistemas de control de acceso personalizado, registrado el paso de las personas por cada zona. Así mismo se ha establecido que el personal visitante tiene que estar permanentemente tutelado por un responsable del centro de datos.

Controles físicos de entrada

Se dispone de un exhaustivo sistema de control físico de personas a la entrada y a la salida que conforman diversos anillos de seguridad.

Se combinan diversos sistemas de seguridad, humanos y técnicos, en la realización de los controles físicos de entrada:

Acceso a la entrada identificándose mediante DNI ante el servicios de seguridad, registrando persona, hora de llegada, salida, autorización que ostenta y dotando de un numero de identificación personal.
Uso del número personal para su identificación ante los dispositivos de seguridad, comprobando autorización y registrando accesos.

Introducción o extracción de equipos

Se requiere autorización expresa del Responsable del Fichero para la realización de estas operaciones, llevando un inventario del material existente y de las entradas y salidas que se han producido.

Cada dispositivo cuenta con un identificador único, descripción, modelo y marca.

5.4.1.b Electricidad y Aire Acondicionado

Las salas donde se ubican los equipos que componen los sistemas de certificación de ANF AC , disponen de suministro de electricidad y aire acondicionado suficiente para crear un entorno operativo fiable. La instalación esta protegida contra caídas de corriente o cualquier anomalía en el suministro eléctrico mediante una línea auxiliar independiente de la fuente eléctrica principal.

Se han instalado mecanismos que mantienen controlados el calor y la humedad a niveles acordes con los equipos que se encuentran instalados en el lugar.

Aquellos sistemas que lo requieren, disponen de unidades de alimentación ininterrumpida y grupo electrógeno,

5.4.1.c Seguridad del cableado

El cableado se encuentra en falso suelo técnico y protegido por medios de detección ante incendio.

5.4.1.d Caja de Seguridad Bancaria

ANF AC ha contratado en una entidad bancaria una caja de seguridad en la que se depositan los instrumentos de emisión de certificados y clave privadas de la CA.

ANF AC ha contratado en una entidad bancaria española una caja de seguridad en la que se depositan copia de los dispositivos que permiten la regeneración del sistema caso de siniestro.

El acceso a la Caja de Seguridad esta restringido a los Directores de Área, los cuales tienen en su poder una de las llaves que permite la apertura de la Caja de Seguridad.

Entre las medidas de protección que poseen estas instalaciones bancarias, reseñar que:

- Las instalaciones cuentan con servicio de vigilancia de 24 horas y control por circuito de televisión interno permanente.

- La arquitectura y blindaje del edificio corresponden al diseño comúnmente empleado en establecimientos denominados “bunker bancario”.

- Las instalaciones se encuentran protegidas constantemente por personal perteneciente a empresa de seguridad autorizada por el correspondiente departamento del Ministerio del Interior.

- El personal al que la entidad bancaria tiene encomendada la administración de los accesos, confecciona un registro del día y hora de entrada y salida, identidad y firma de la persona que accede.

- El acceso al núcleo central se realiza superando distintos controles. El personal que accede se encuentra en todo momento acompañado por el personal responsable de la administración del “bunker bancario” y la operación de apertura de la caja bancaria se realiza mediante doble llave: una en poder del personal de *ANF AC* y otra en poder del personal de la entidad bancaria.

- Todas las instalaciones cuentan con sistemas de energía y aire acondicionado, que cumplen con las normas al efecto

- Todas las instalaciones cuentan con mecanismos de prevención y protección contra incendios. Dichos mecanismos cumplen con las normas industriales.

5.5 Seguridad criptográfica.

Comunicaciones

La infraestructura de clave pública *PKI* de ANF AC cuenta con un sistema de comunicaciones "Secure Sockets Layer" SSL de 128 bits.

Longitud de Clave certificados

La clave de firma de ANF AC tiene una longitud de 2048 bits.

Los Pares de Claves de firma de los usuarios de ANF AC están especificados en su respectiva de Política de Certificación.

Algoritmos

Los algoritmos de "función resumen" utilizados en la emisión de certificados, quedan especificados en el apartado correspondiente.

En cuanto al algoritmo SHA-1 que en la actualidad se encuentra en situación de "riesgo", podrá mantener su vigencia en tanto en cuanto permanezca su actual valoración. Los certificados y las firmas en las que haya intervenido este algoritmo SHA-1 perderán su vigencia al cambiar su valoración a "no seguro" o "no autorizado".

Respecto al algoritmo SHA-2, ANF AC ya lo utiliza en determinados certificados y servicios de certificación. P.e. Servicio de Sellado Digital de Tiempo. Este algoritmo sustituirá en su momento al SHA-1

El estado de vigencia en el que se encuentran los algoritmos empleados por ANF AC , es publicado en la URL :

http://www.anf.es/AC/algoritmos/

Los procedimientos técnicos y los algoritmos utilizados quedan ampliamente documentados en el Anexo IV.

Contraseñas de acceso a los servicios Web por parte de los usuarios

Las contraseñas son almacenadas de forma ininteligible al encontrarse cifradas.

Las contraseñas tienen un periodo de vigencia de tres meses, los usuarios deben de modificarlas antes de su caducidad.

En caso de caducidad u olvido, el sistema le permite introducir una nueva contraseña mediante el sistema de preguntas-respuestas (3, 100 % de acierto)

Datos de generación de firma

ANF AC , no almacena ni copia los datos de creación de firma de sus usuarios, ni tiene oportunidad para hacerlo, estos son generados de forma independiente por ellos mismos y sin intervención de terceros.

Generación certificado petición y contenedor de claves

El dispositivo entregado al suscriptor confecciona un “certificado de petición”, el cual es firmado electrónicamente con la clave privada. El “certificado de petición” queda construido en formato PKCS#10 y debe de ser transferido a los servidores de certificación de ANF AC .

La Clave Privada esta custodiada en un módulo criptográfico PKCS#15 v.1.1 que reúne el nivel de seguridad requerido por la norma de referencia europea CEN CWA 14169.

Acta de identificación

El acta de identificación generada por la Autoridad de Registro Reconocida, se elabora mediante un software criptográfico construido bajo el modelo PKCS#15 v.1.1. Para acceder a esta información se precisa el empleo de la librería criptográfica de ANF AC .

Para acceder a la información contenida en el token criptográfico se requiere la activación mediante contraseña secreta, la lectura se efectúa en modo protegido. Se accede a los datos mediante un hilo de acceso exclusivo, y en ningún momento se escribe la información en disco.

La contraseña secreta de activación es generada por el dispositivo AR Manager mediante generación aleatoria.

Cada acta de identificación esta asociada a un Localizador AR único y exclusivo. El acta de identificación es publicada en el Registro General, siendo accesible mediante el Localizador AR.

Cada Acta de Identificación esta asociada a un Localizador AR único y exclusivo. El Acta de Identificación (sin las propiedades de activación), es publicada en el Registro General, siendo accesible mediante el Localizador AR.

Los certificados electrónicos incluyen la URL de publicación del Acta de Identificación y la firma electrónica de la ARR.

Acceso al código fuente

Este PSC con el fin de facilitar un control completo a sus usuarios del software utilizado en los procesos anteriormente reseñados, facilita la revisión del código fuente del software criptográfico y de las aplicaciones empleadas en la generación de Datos de creación de firma, creación y transmisión del certificado de petición en formato PKCS#10, creación del token criptográfico construido siguiendo el formato PKCS#15 que contiene el Acta de Identificación.

Dado que el software utilizado por los usuarios de ANF AC cuenta con mecanismos que garantizan la integridad y autenticidad de todos los elementos que conforman su plataforma de trabajo, no se autoriza la modificación del código fuente, aunque aquellos usuarios que lo deseen podrán requerir del departamento técnico de ANF AC que la generación de los dispositivos se realice sobre el código que han revisado y en su presencia. ANF AC aplicará las tasas correspondientes al servicio de ingeniería prestado.

Dispositivo RDE

El dispositivo empleado por el Responsable de Dictámenes de Emisión tiene la capacidad de verificar automáticamente la integridad de los datos contenidos en el certificado de petición, así como la correspondencia de los datos que figuran en el

certificado con el acta de identificación realizada por la Autoridad de Registro Reconocida.

Sistema de Generación de los certificados

Este sistema afecta al tratamiento de los datos personales de los usuarios de ANF AC . Este sistema se ha desarrollado siguiendo las normas

RFC 5280
RFC 3039
ETSI TS 101862 v 1.2.1
Orden HAC 1181/2003

Los datos incorporados en los certificados, son los expresamente requeridos por la legislación vigente y aquellos que, de forma expresa, ha solicitado su titular.

Descarga del certificado emitido

El dispositivo criptográfico con el que ha sido dotado el usuario tiene la capacidad de descargar automáticamente el certificado emitido a través de canal seguro SSL v.3. Antes de ser cargado en el contenedor de certificados de ANF AC , el sistema procede a verificar automáticamente que el certificado emitido por ANF AC contiene la clave pública que corresponde a la clave privada que esta en posesión del titular.

Dispositivo de creación de firma electrónica

Todos los componentes utilizados por los Dispositivos homologados de Creación de Firma Electrónica (en adelante Dispositivo), se encuentran bajo el control de *ANF AC,* bien porque han sido desarrollados por el propio Departamento de I+D, o bien porque se ha revisado el código fuente, supervisando su compilación final y autentificando mediante firma electrónica. Ello permite garantizar un nivel homologado de seguridad de acuerdo con los requerimientos establecidos en la Política de Firma Electrónica de este *PSC* :

Estos dispositivos cumplen las normas técnicas reseñadas en el apartado “Normas y Estándares” de este documento,

Información general

Toda la información relativa al software criptográfico, código fuente de la librería criptográfica y documentación de procedimientos puede ser descargada en la URL.

https://www.anf.es/AC/documentos/

Con el fin de garantizar la integridad y autenticidad de estos ficheros, todos ellos se encuentran firmados electrónicamente. Para su verificación se puede descargar gratuitamente el dispositivo de verificación en la URL

https://www.anf.es/AC/dispositivos/

Los procedimientos criptográficos utilizados por ANF AC han sido revisados por especialistas en la materia, y de forma periódica es revisada su calidad y su resistencia en lo que a seguridad se refiere. Las certificaciones acreditativas independientes son publicadas en la URL

https://www.anf.es/AC/documentos/

ANF AC mantiene un departamento de criptoanálisis dedicado a analizar la evolución de toda aquella tecnología que pueda afectar a la seguridad de los sistemas de certificación empleados por ANF AC . De acuerdo con la información obtenida, el responsable del departamento podrá activar:

Vigilancia activa nivel 1

Afecta elementos críticos del sistema de certificación. A modo meramente enunciativo: *algoritmos de firma, funciones de resumen o longitud de claves de creación de firma*.

Consulta de nuevas noticias que puedan relacionarse con la cuestión sujeta a vigilancia en foros criptográficos y buscadores generales. Esta labor se realiza semanalmente.

Vigilancia activa nivel 2

Cualquier otro elemento que aunque perteneciente al sistema de certificación, no es catalogado como crítico.

El procedimiento de vigilancia y la periodicidad queda a criterio del responsable del departamento.

Plan de Contingencias –criptografía-

Se confirma la existencia de un riesgo cierto.

Se activa inmediatamente el Plan de Contingencias y se procede de acuerdo con lo estipulado en el mismo.

5.6 Seguridad a la adecuación a las disposiciones legales.

ANF AC de cada nueva publicación que realiza de sus documentos de prácticas de certificación, solicita un informe jurídico a fin de determinar la correcta adecuación de los mismos a las disposiciones legales vigentes.

ANF AC cuenta con servicios jurídicos que velan por la permanente adecuación de sus prácticas de certificación a las disposiciones legales vigentes. Caso de producirse alguna novedad legislativa o reglamentaria que afecte al sistema PKI de ANF AC , los servicios jurídicos están instruidos para que de oficio eleven a la Junta Rectora de la PKI la correspondiente propuesta de modificación que permita adecuarlos a las nuevas necesidades.

5.7 Seguridad de la adecuación de la *DPC* a las Políticas de Certificación.

No se pueden realizar cambios que no sean soportados por las CP's asociadas. Deben, en todo caso, contemplarse simultáneamente con actualizaciones de las CP's afectadas.

La Junta Rectora de la PKI de *ANF AC* es la entidad que determina la adecuación de esta *DPC* de ANF AC con las que políticas de certificación con las que se relaciona.

5.8 Control de conformidad.

ANF AC realiza periódicamente auditorías que controlan el correcto cumplimiento de cada uno de los apartados de Seguridad. Los procedimientos y frecuencia para la realización de auditorías están regulados en el reglamento interno de la

Seguridad Administrativa de *ANF AC*; los criterios seguidos para la definición de los procedimientos de auditoría se encuentra detallados en el ANEXO III.

5.9 Otros documentos de Seguridad.

- Política de Seguridad
- Análisis de Riesgos
- Plan de Contingencias

Puede ser consultado en la URL:

https://www.anf.es/AC/documentos/

5.10 Procedimiento de revisión.

El Responsable de Seguridad, asume la responsabilidad de mantener en todo momento actualizado el Documento de Seguridad. Debiendo revisarlo siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, deberá adecuarlo, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Antes de aplicar cualquier modificación al Documento de Seguridad, deberá informar y solicitar la autorización expresa del Responsable del Fichero, adjuntando además una relación del personal cuyas funciones se pueden ver afectadas por los cambios propuestos.

En caso de autorización por parte del Responsable del Fichero, el Responsable de Seguridad será el encargado de organizar la efectiva aplicación de las modificaciones introducidas en el Documento de Seguridad, así como de trasladar y crear, en caso de necesidad, el correspondiente proceso de formación a los usuarios. En cualquier caso, siempre se notificará de las modificaciones realizadas, y se requerirá del personal que firme el correspondiente acuse de recibo.

6. Normas y Estándares.

6.1 Normas internacionales

Los sistemas de certificación de ANF AC siguen la normas que figuran en la URL

http://www.anf.es/AC/normas/

6.2 Homologación de dispositivos por ANF AC .

Con el fin de garantizar a la comunidad de usuarios de esta PKI, unos niveles básicos de seguridad y calidad, se pone a su disposición una serie de dispositivos homologados por ANF AC. Los dispositivos que comprende este apartado son:

- Dispositivo de creación de firma.
- Dispositivo de verificación de firma.
- Dispositivo de generación de datos de creación de firma.
- Dispositivo de generación del contenedor.

Cualquier entidad podrá solicitar de ANF AC la homologación de los dispositivos por ella desarrollados.

Se procederá a otorgar la homologación solicitada cuando el dispositivo cumpla:

- Lo establecido en la legislación vigente.
- Los criterios y procedimientos reseñados en este documento, sus Anexos y Políticas de Certificación.
- Ser operacionalmente compatibles con el resto de dispositivos homologados por *ANF AC*.
- Informe favorable del Departamento Técnico de ANF AC.
- Los dispositivos de creación de firma deben cumplir las especificaciones técnicas en materia de Dispositivos Seguros de Creación de Firma Electrónica.

La propia evolución de los servicios de certificación de ANF AC, puede conllevar la necesidad de adaptar los dispositivos homologados a los nuevos requerimientos que se establezcan en virtud de la emisión de actualizaciones de esta DPC, sus Anexos y Políticas de Certificación.

Los nuevos criterios serán siempre objetivos, sobre la base de requerimientos de carácter legal, que presupongan una mejora en la prestación de los servicios de certificación o atiendan a una necesidad de seguridad técnica. En caso de producirse nuevos criterios de homologación, todos los dispositivos homologados deberán adaptarse, o en su caso, ANF AC deberá retirarles la homologación otorgada.

Los dispositivos homologados están publicados en la URL:

https://www.anf.es/AC/dispositivos/

6.3 Dispositivos seguros de creación de firma electrónica.

ANF AC exclusivamente homologa dispositivos de creación de firma electrónica que cumplen con los requerimientos establecidos en las normas y estándares internacionales sobre dispositivos de creación de firma de larga duración. A modo meramente enunciativo se garantiza que los dispositivos homologados por ANF AC, cumplen con los siguientes requerimientos:

- Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.
- El dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.
- Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
- 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.

- Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
- 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.
- Que el dispositivo previa a la utilización de los datos de creación de firma, establece conexión con el servidor de ANF AC a fin de comprobar el estado en que se encuentra el certificado del usuario. Denegando el servicio de firma si el certificado esta caducado o revocado.
- Que el dispositivo para cada firma electrónica que procesa, requiere del Servicio de Sellos de Tiempo de ANF AC , que le sea generado un Sello de Tiempo único y exclusivo sobre la firma electrónica que ha creado.

En Anexo IV de esta DPC queda documentado técnicamente el procedimiento seguido por los dispositivos de creación de firma homologados por ANF AC, y los algoritmos criptográficos que se emplean.

6.4 Dispositivo de verificación de firma.

Los dispositivos desarrollados por ANF AC para la verificación de firma electrónica pueden ser descargados y utilizados de forma gratuita, a través de la URL:

https://www.anf.es/AC/dispositivos/

siendo de libre distribución.

ANF AC garantiza que exclusivamente desarrolla y homologa dispositivos de verificación de firma que cumplen con los requerimientos básicos establecidos por la legislación vigente:

- Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.
- Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

- Los dispositivos de verificación de firma electrónica homologados por ANF AC garantizan, que el proceso de verificación de una firma electrónica y de los certificados emitidos por esta AC satisface, al menos, los siguientes requisitos:
- Que los datos utilizados para verificar la firma corresponden a los datos mostrados a la persona que verifica la firma.
- Que la firma se verifica de forma fiable y el resultado de esa verificación se presenta correctamente y de forma legible y entendible.
- Que la persona que verifica la firma electrónica puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.
- 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.
- Que se verifican de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.
- Que se detecta cualquier cambio relativo a su seguridad.

Asimismo, si la firma ha sido creada con un dispositivo de creación de firma electrónica homologado por ANF AC, se verifica la integridad del *Timestamping* y la identidad de ANF AC TSA como firmante del *Timestamping*.

Los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, pueden ser almacenados u obtenidos directamente de ANF AC , por la persona que verifica la firma electrónica, si así lo desea.

6.5 Dispositivo de generación de datos de creación de firma.

ANF AC , no genera los datos de creación de firma de sus usuarios. Esta AC pone a disposición de sus usuarios el dispositivo de generación de datos de creación de firma, quedando así plenamente garantizada la confidencialidad del proceso. Así mismo, y con el fin de facilitar un control completo a sus usuarios del software utilizado en el proceso anteriormente reseñado, facilita, caso de ser requerida, revisión del código

fuente del software criptográfico y de determinadas aplicaciones de acuerdo con lo reseñado en el apartado “Seguridad Criptográfica” de este documento.

6.6 Dispositivo de generación del contenedor.

Los datos de creación de firma únicamente pueden ser almacenados en contenedores homologados por ANF AC. Esta Autoridad de Certificación ha homologado los publicados en la URL:

https://www.anf.es/AC/contenedores/

La Clave Privada esta custodiada en un módulo criptográfico que reúne un nivel de seguridad igual o superior al establecido por la norma de referencia europea CEN CWA 14169.

6.7 Sistemas de certificación.

ANF AC en el diseño y elaboración de sus sistemas de certificación, sigue y respeta las especificaciones técnicas elaboradas al efecto por los organismos internacionales, se puede obtener detalle de las normas seguidas en la URL

http://www.anf.es/AC/normas

6.8 DPC, Anexos y Políticas.

Las siguientes leyes y normas han sido consideradas para la elaboración de estos documentos:

Directivas europeas

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1.995. Relativa a la Protección de Datos de las Personas Físicas.

- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de Diciembre de 1.997. Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- Directiva 99/93/CE del Parlamento Europeo y del Consejo, de 13 de Diciembre de 1.999. Por la que se establece un marco comunitario para la firma electrónica.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Legislación ámbito ANF AC

- Real Decreto 994/1999, de 11 de Junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.
- Ley 59/2003, de 19 de Diciembre de 2.003, de Firma Electrónica
- La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.
- Ley 34/2002,de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico
- Orden HAC 1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la *Agencia Estatal de Administración Tributaría.*

Normas

Las reseñadas en:

http://www.anf.es/AC/normas

7. Certificados electrónicos.

Esta sección especifica las características de todos los certificados emitidos por ANF AC. Para una mejor comprensión del lector, la información se ha dividido en dos apartados:

1.- Certificados raíz y Certificados de autoridades intermedias.
2.- Certificados de entidad final.

Los certificados respetan el formato definido por la UIT –T X-509, de fecha junio 1.997 o superiores (de referencia ISO/IEC 9594-8 de 1997) en la versión 3.

Las Listas de Revocación CRL's siguen el perfil propuesto en la recomendación UIT-T X-509, en su versión 2.

El servicio Online Certificate Status Protocol (OCSP) sigue las recomendaciones establecidas en la norma RFC 2560.

7.1 Certificados de ANF AC autoridad intermedia

Este tipo de certificados solo pueden ser emitidos por orden expresa de la Junta Rectora de ANF Autoridad de Certificación, matriz de ANF AC. La cual procederá bajo alguna de las siguientes cuestiones:

- Una Autoridad Intermedia por cada tipo de certificado a emitir, cada tipo de certificado a emitir irá acompañado de sus políticas de certificación que especificarán sus características y particularidades.

- Por motivos de seguridad y para evitar grandes daños en caso de vulneración de una clave. Concretamente se emitirá un nuevo certificado de Autoridad al haber emitido 10.000 certificados con un determinado certificado de Autoridad Intermedia.

- Una Autoridad Intermedia por cada filial de ANF AC.

7.1.a Proceso de Generación de las Claves.

Este *PSC* garantiza que:

- Los datos de creación de firma se generan en un ambiente de seguridad, directamente controlado por personal de alta dirección de *ANF AC*.
- La generación de los datos de creación de firma se realiza bajo supervisión de todos los operadores autorizados en la orden de emisión, el Presidente de la Junta Rectora de *ANF AC* es el responsable de verificar la identidad de todos ellos.
- La generación de los datos de creación de firma se han realizado dentro de un módulo criptográfico que reúne los requisitos FIPS 140-1 nivel 3.

El proceso seguido para la generación de las claves y la emisión de los certificados, quedan registrados en un Acta que a tal efecto es levantada durante la Ceremonia de Generación.

7.1.b Protección de las Claves Privadas.

Controles de Seguridad de la Clave Privada:

La Clave Privada esta custodiada en un módulo criptográfico que reúne el nivel de seguridad requerido por la norma de referencia europea CEN CWA 14169 equivalente a ISO 15408 Common Criteria EAL 4+

El acceso a los módulos criptográficos esta restringido a personal autorizado de ANF AC, se realiza en todo momento de forma dual y en presencia de un responsable del departamento de seguridad del Centro de Datos.

La clave esta vinculada al equipo informático que la contiene, no siendo posible su activación en otro ordenador. Este material esta depositado en caja de seguridad de bunker bancario.

Los dispositivos de activación del software y del hardware se encuentran en poder de los operadores autorizados, y la activación de los dispositivos requiere la

presencia simultánea de al menos dos de los operadores autorizados y la supervisión de un responsable de seguridad del Centro de Datos.

El ordenador se encuentra ubicado en instalaciones de alta seguridad que cumplen las especificaciones reseñadas en el apartado "*Seguridad física*" de este documento.

Otras características relevantes del equipo dedicado a la emisión de certificados:

a) El ordenador no esta conectado a Internet, ni a una Intranet. Salvo en el momento de uso, esta desconectado de la corriente eléctrica. En el momento de uso el flujo eléctrico es adquirido de un batería, a fin de impedir desperfectos por fluctuaciones eléctricas.
b) El ordenador gestiona un registro en el que consta el momento de activación y desactivación del sistema.
c) El ordenador se encuentra precintado con etiquetas de seguridad. Las laborares de mantenimiento se realizan en presencia de al menos dos responsables de ANF AC .

7.1.c Copia de seguridad de las Claves Privadas.

ANF AC con el fin de garantizar la continuidad del sistema ante cualquier posibilidad de siniestro, ha depositado en Caja de Seguridad bancaria española, una copia de las Claves Privadas y de los Token que permiten su activación. Antes de guardarse en el contenedor de transporte, las claves han sido cifradas bajo triple clave y se ha custodiado durante todo el trayecto por dos altos cargos de ANF AC .

7.1.d Objetivos de uso de las Claves Privadas.

ANF AC hace uso exclusivo de las Claves Privadas para los fines que fueron generadas.

7.1.e Certificados raíz.

ANF AC como Prestador de Servicios de Certificación matriz de esta *PKI*, dispone un certificados raíz (autofirmado con sus respectivas clave privada) con los que

firma los certificados de clave pública de autoridad intermedia de ANF AC que a su vez, emplean sus claves privadas para firmar los certificados de las entidades finales, o según tipo de certificado, firmando directamente los certificados de entidad final. De este modo toda la organización o jerarquía se encuentra cubierta por la confianza del certificado raíz del *ANF AC* con nombre:

ANF Server CA

Para garantizar la confianza de todos los certificados de la jerarquía ANF Server CA, se publican los certificados firmados y las respectivas Listas de Certificados Revocados en un servidor accesible a todos los terceros de confianza interesados en verificar las validez de los mismos, además este PSC dispone de otros instrumentos de verificación de alta disponibilidad, como por ejemplo el servicio OCSP, o SOAP.

Cada certificado incorpora un número de serie único independientemente de su tipo.

7.1.f Certificados de autoridad intermedia

Bajo la jerarquía ANF Server CA se crearán autoridades intermedias con el objetivo de facilitar la gestión del sistema y evitar la concentración de grandes volúmenes de certificados bajo un mismo nodo, minimizando de esta forma riesgos de seguridad.

7.1.g Cambio de los Certificados.

ANF AC procede al cambio de sus certificados en los siguientes casos:

7.1.g.1 Fin del Ciclo de Vida de los certificados.

ANF AC maneja todos los aspectos relativos al cambio de claves. Cuando se haya superado cuatro quintos del tiempo de vida del certificado de la Autoridad de Certificación, se generará uno nuevo.

Los certificados sustituidos son revocados bajo el concepto de “cese de operaciones” . En este supuesto:

- Se realiza un informe del cambio de certificados, remitiéndolo a la Junta Rectora de la PKI.
- Todas las copias y fragmentos de la clave privada de *ANF AC* se destruyen.
- Se procede a la revocación de todos los certificados que han sido emitidos utilizando el Certificado CA revocado.

7.1.g.2 Fin del Ciclo de Vida del hardware que contiene el modulo criptográfico.

Finalizado el Ciclo de Vida del hardware, ya sea por fallo fortuito, obsolescencia del equipo o simple proceso de caducidad prevista en el plan de seguridad, se procede a la destrucción de los certificados vinculados a este dispositivo.

7.1.g.3 Fin del ciclo de Vida de los componentes criptográficos.

ANF AC mantiene un seguimiento de la seguridad de los certificados en términos criptográficos. Caso de tener conocimiento o sospecha cierta de debilidad en alguno de los elementos sobre los que se sustenta el sistema, se procede al cambio de estado y a la activación del Plan de Contingencias.

Según la incidencia detectada, el estado puede ser: “en riesgo” o “no seguro”.

El concepto de revocación de los certificados afectados por un cambio de estado a “no seguro”, queda clasificado como “Cese de elementos criptográficos”, y no estará autorizado su uso en el ámbito de la PKI de *ANF AC* . En este supuesto:

- Se realizará un informe del cambio de certificados, remitiéndolo a la Junta Rectora de la PKI.
- Todas las copias y fragmentos de la clave privada de *ANF AC* se destruyen.

- Se procede a la revocación de todos los certificados que han sido emitidos utilizando el Certificado CA revocado.

Los elementos sobre los que se establece un control permanente de seguridad son:

- Algoritmo de generación de Hash.
- Algoritmo de generación de Firma.
- Longitud de la Clave Privada.

7.1.g.4 Rotura de Seguridad de la Clave Privada.

ANF AC mantiene máximos niveles de seguridad sobre sus sistemas de certificación, no obstante se debe de tener en consideración la posibilidad de que pueda producir un supuesto de rotura de seguridad de este elemento, en cuyo caso, *ANF AC* procede a la revocación inmediata del Certificado, conceptuando dicha revocación como “Rotura de Seguridad”.

Se procede a la parada de los servicios de certificación y se activa el Plan de Contingencias.

En todos los supuestos:

- Se realizará un informe del cambio de certificados, remitiéndolo a la Junta Rectora de la PKI.
- Todas las copias y fragmentos de la clave privada de *ANF AC* se destruyen al finalizar el ciclo de vida.
- Se procede a la revocación de todos los certificados que han sido emitidos utilizando el Certificado CA revocado.

7.1.h Difusión.

Los certificados de *ANF AC* son de acceso público, sin restricción alguna. Se encuentra publicado en la URL:

https://www.anf.es/AC/repositorio/

El certificado de *ANF AC* se incluye en los dispositivos de creación de firma electrónica y se instala automáticamente con cualquiera de los dispositivos homologados de esta AC.

7.1.i Destrucción de la Clave Privada.

Una vez finalizado el ciclo de vida de las claves privadas, *ANF AC* procede a su destrucción y a la destrucción de cualquier copia de las mismas, siguiendo procedimientos que imposibilitan su recuperación.

7.1.j Periodo de validez

El periodo de validez de los certificados empleados por *ANF AC* en el desarrollo de su actividad, es el adecuado al tipo de algoritmo escogido y a la longitud de la clave según normas internacionalmente aceptadas.

El periodo de validez de cada certificado queda especificado en el apartado "Perfiles del certificado"

7.1.k Ciclo de vida del hardware que contiene modulo criptográfico.

Se garantiza la seguridad del hardware criptográfico a lo largo de su ciclo de vida.

En particular se responsabiliza que:

- *no puede ser manipulado durante su actividad operacional, cualquier labor de mantenimiento requiere una parada previa del módulo criptográfico;*
- *la instalación, activación y administración del hardware se realiza por personal especialmente autorizado de acuerdo con los roles definidos por ANF AC . Siempre bajo presencia dual y además, siendo supervisado por un responsable del área de seguridad;*
- *el hardware y el modulo criptográfico funcionan correctamente ; y*
- *finalizado el ciclo de vida, las claves son borradas siguiendo procedimientos que imposibilitan su recuperación.*

7.1.I Perfiles del Certificado .

7.1.I.a Perfiles del Certificado.

Números de versión soportada

Soporta y emite certificados X. 509 versión 3.

OID del algoritmo criptográfico

OID de los algoritmos criptográficos utilizados en la jerarquía de:

ANF Server CA

Sha1RSA: **1.2.840.113549.1.1.5**

Formas de nombres

Se ha establecido una sola jerarquía de nominación, sobre la base del formulario de Nombre Distintivo.

Perfil básico del Certificado de ANF Server CA	
Versión	v3
Número de Serie	01 34 4b
Algoritmo de firma	Sha1RSA
Emisor	CN = ANF Server CA Número de serie = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificación L = Barcelona (see current address at https://www.anf.es/address/) S = Barcelona C = ES
Válido desde	martes, 01 de diciembre de 2009 0:00:00
Válido hasta	miércoles, 01 de diciembre de 2021 0:00:00
Asunto	CN = ANF Server CA Número de serie = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificación L = Barcelona (see current address at https://www.anf.es/address/) S = Barcelona C = ES
Clave Pública	RSA (2048 Bits) 30 82 01 0a 02 82 01 01 00 bf ea 48 a7 9a 88 39 6b 2c 48 40 07 04 93 7c f7 b8 2d 7e a5 37 e2 61 d6 21 fc 90 37 cb 69 3e 5e 8b 37 df 5b 6f 3b d8 b6 c3 88 40 90 f4 9d 0c 5c 10 52 b1 b3 e5 5f 91 10 e6 fd a8 80 14 5f d3 8b bd 5c bd 0f 23 92 09 37 e3 72 d2 66 94 0b 5c 74 94 2f 5e f2 4e d8 03 c6 b3 ce 56 a5 1c d9 7b fd 4f 07 4c d4 b7 da 5f 29 4d 75 f2 1f 55 cf 32 23 1c 46 09 27 1d 45 ec f1 8c 34 89 de 7b 16 a7 43 5e 8a 2b e9 94 43 1e d7 3e 93 6d 6f 89 3d bc ee b1 c8 b7 ff c9 7d e3 5f 0d 6f 77 78 f5 2a 2e 8d c4 8b 98 97 30 b1 46 5a 0b 63 70 d4 78 c7 86 b3 7f ff 27 42 aa 9f 8a 6e 6d a1 94 ca ec 87 02 1c d6 54 4b fd bc 89 9b a6 63 38 66 8c 16 89 89 97 c3 50 e8 f6 42 01 a7 77 7d 10 19 92 03 e8 5d 45 c8 15 c5 87 1b 0d 91 f2 c6 39 9c 7b f3 c0 0a 99 f8 ee 83 6f 7e 42 77 11 8e c3 1f 1c 72 2f 3d 1b 02 03 01 00 01

Restricciones básicas	Tipo de asunto=Entidad emisora de certificados (CA) Restricción de longitud de ruta=Ninguno
Uso de la clave	Firma de certificados, Firma CRL sin conexión, Firma CRL (06)
Nombre alternativo del sujeto	Nombre RFC822=ac@anf.es
Huella digital	12 61 25 c5 7d b7 7b 9d a8 47 d9 0d 6c 3e 9f 8a d0 f7 c0 1e

7.1.I.b Perfiles de la CRL.

Las CRL son firmadas con un certificado que ha sido emitido por la PSC raíz de la jerarquía.

Números de versión soportada

Soporta y emite certificados X. 509 versión 2.

Extensiones de los certificados

Definidos en su respectiva CP.

OID del algoritmo criptográfico

OID de los algoritmos criptográficos utilizados en la jerarquía de:

ANF Server CA

Sha1RSA: **1.2.840.113549.1.1.5**

7.2 Certificados de entidad final

ANF AC realiza todos los trámites necesarios para garantizar de forma fiable la veracidad de los datos contenidos en cualquier certificado antes de su activación. En certificados en los que el usuario haya consignado un seudónimo, *ANF AC* garantiza que ha constatado de forma fiable su verdadera identidad y conserva la documentación que lo acredita.

Los certificados emitidos bajo seudónimo, reseñarán previo al nombre elegido por el usuario, la reseña "seudónimo". Idéntica reseña se insertará en aquellos apartados que permiten asociarlo con la identidad cierta del usuario, p.e. *DNI – NIF - eMail*

ANF AC garantiza la confidencialidad y privacidad de sus usuarios. Sus datos personales son sólo accesibles por personas por ellos autorizadas.

ANF AC no emitirá un certificado sin el consentimiento de su titular. El consentimiento para la emisión se entiende prestado desde el momento en que se realiza la solicitud del certificado, y se suscribe el correspondiente Contrato de Prestación de Servicios de Certificación.

ANF AC se reserva el derecho a negarse a emitir un certificado, a su libre discreción, sin incurrir en responsabilidad alguna por cualquier pérdida o lucro cesante que pueda producir tal negativa.

Los certificados de *ANF AC* únicamente pueden ser solicitados por personas mayores de edad, para ser utilizados en su propio nombre, o en representación de terceras personas físicas o jurídicas. La generación de los datos de creación de firma por parte del usuario, y la tramitación de la correspondiente solicitud del certificado, supone su aceptación y consentimiento para la emisión del certificado por parte de *ANF AC* .

Cada certificado emitido por *ANF AC* esta asociado a una Política de Certificación determinada, a la cual esta sometido el titular y los representantes que hacen uso del mismo.

Son propietarios de estos contenedores, las personas físicas o jurídicas a las que representa la persona física autorizada a utilizar el certificado o, caso de actuar en su propio nombre, el propio usuario.

Las Políticas de Certificación asociadas a los certificados emitidos por *ANF AC* determinan el contenedor que debe usarse en cada tipo de Certificado.

7.2.a Dispositivo de Generación del Contenedor.

ANF AC facilita este dispositivo, el cual tiene la capacidad de generar el contenedor que almacena los datos de creación de firma.

La distribución esta restringida a las *ARR*.

7.2.b Generación de datos de creación de firma.

Las claves de los usuarios se generan bajo su exclusivo control utilizando los instrumentos que *ANF AC* pone a su disposición. No se precisa la intervención de ningún tercero, exclusivamente el titular tiene acceso a los datos de creación de firma, y decide personalmente el PIN de activación.

El dispositivo debe de estar homologado por *ANF AC* .

7.2.c Difusión del dispositivo de generación de datos de creación de firma.

ANF AC pone a disposición de sus usuarios el dispositivo de generación de datos de creación de firma electrónica.

La distribución esta restringida a las Autoridades de Registro Reconocidas, las cuales tras efectuar el correspondiente proceso de identificación y autentificación, hacen entrega del dispositivo, facilitando al usuario un acta de identificación, contraseña de activación del acta, y un identificador denominado “Localizador AR”.

El Localizador AR permite al suscriptor determinar la situación en que se encuentra en cada momento su solicitud. No obstante, cuando el proceso de identificación y autentificación se ha llevado a cabo ante Autoridades de Registro Colaboradoras, *ANF AC* será la encargada de hacer entrega del dispositivo enviándolo por correo certificado o mediante descarga telemática a través de un servidor seguro SSL.

Las actualizaciones de los dispositivos a las nuevas versiones autorizadas por *ANF AC* , se realizan de forma automática a través de Internet.

7.2.d Instalación del dispositivo.

El usuario de *ANF AC* debe de proceder a la instalación del dispositivo siguiendo sus instrucciones técnicas.

7.2.e Procedimiento de generación de datos de creación de firma.

El usuario en posesión del acta de identificación y del dispositivo de generación de datos de creación de firma, esta en disposición de generar su par de claves de firma y el certificado de petición personalizado. Este proceso lo realiza personalmente y sin mediación de terceros, de forma automática y mediante la simple selección del PIN que será la contraseña secreta de activación.

De este modo el usuario, tras activar el acta de identificación, selecciona de forma autónoma cual va a ser su PIN de activación de firma, y decide el momento de generar los datos de creación de firma. Este PIN debe de tener una longitud

mínima de 8 dígitos alfanuméricos, y se puede llegar a denegar un PIN propuesto si el sistema lo considera inseguro, el dispositivo cuenta con una biblioteca de claves no autorizadas.

El programa genera el par de claves, y construye el certificado de petición correspondiente a las claves creadas, debidamente personalizado con los datos integrados en el acta de identificación. Los datos de creación de firma quedan contenidos en un token software criptográfico que sigue el formato PKCS#15v1.1.

ANF AC no almacena ni copia los datos de creación de firma de sus usuarios, ni tiene oportunidad para hacerlo.

Los datos de generación de firma son introducidos automáticamente en uno de los contenedores homologados por *ANF AC* y autorizado por la Política de Certificación asociada a ese certificado.

7.2.f Certificado de petición.

Procedimiento establecido:

a) Queda construido en formato PKCS#10.
b) Contiene el Localizador AR asociado al Acta de identificación expedida por la *ARR*, los datos básicos del usuario y su clave pública.

El fichero es firmado por el usuario con su clave privada, es cifrado y queda listo para su envío a *ANF AC* .

7.2.g Modalidades de certificados.

En la definición de los tipos de atributos se sigue la recomendación UIT-T x-520 de referencia en la ISO/IEC 9594-6

Bajo cualquiera de los nodos de la jerarquía ANF Server CA, se pueden emitir certificados de test para realizar pruebas técnicas. Estos certificados se emiten teniendo como titular información que indique que se trata de una prueba sin valor.

7.2.i Perfiles del Certificado y CRL.

7.2.i.a Perfiles del Certificado.

Todos los certificados de entidad final están de conformidad con el estándar X-509 v.3 .

Las CRL son firmadas con un certificado que ha sido emitido por la PSC raíz de la jerarquía correspondiente.

Números de versión soportada

Soporta y emite certificados X. 509 versión 3.

Extensiones de los certificados

Definidos en su respectiva CP.

OID del algoritmo criptográfico

Los OID de los algoritmos criptográficos utilizados son:

Certificados de entidad final emitidos baja loa jerarquía ANF Server CA.

Sha1RSA: **1.2.840.113549.1.1.5**

7.2.i.b Perfiles de la CRL.

Números de versión soportada

Soporta y emite certificados X. 509 versión 2.

Extensiones de los certificados

Definidos en su respectiva CP.

OID del algoritmo criptográfico

Los OID de los algoritmos criptográficos utilizados son:

SHA1RSA: **1.2.840.113549.1.1.5**

7.2.j Identificación y autenticación.

Este apartado se desarrolla de manera específica para cada tipo de certificado a través de su respectiva Política de Certificación.

De forma general se establece:

7.2.j.1 Tipos de nombres.

ANF AC ha establecido una sola jerarquía de nominación para cada usuario, sobre la base del formulario de Nombre Distintivo "DN" conforme a las recomendaciones X.501 de referencia en la ISO/IEC 9594-2.

El DN contiene como mínimo los siguientes elementos:

- Componente Nombre (Common Name) –CN
- Componente dirección correo electrónico (E-mail) –E
- Componente de ubicación geográfica –ST
- Componente de Estado (Country) –C
- Componente de número de serie –serialNumber
- Componente nombre de pila (GivenName) -G

Las reglas utilizadas para interpretar varios formatos de nombres son las establecidas en la recomendación x-500.

7.2.j.2 Seudónimo.

Cuando la *CP* del certificado solicitado permita expresamente el empleo de seudónimos, los usuarios podrán solicitar de *ANF AC* que el certificado sea emitido con un seudónimo.

Podrá ser rechazado por la *ARR* seudónimos que, por similitud a otros ya existentes puedan inducir a confusión; así mismo se podrán rechazar seudónimos peyorativos, de carácter grosero, que correspondan a marcas comerciales conocidas o cuyo significado se considere inadecuado.

7.2.j.3 Unicidad de nombres.

Los nombres distinguidos serán únicos para cada suscriptor.

La información es integrada en los certificados en formato UTF-8, algunos nombres acentuados pueden ser leídos de forma incorrecta en determinados sistemas operativos comerciales.

7.2.j.4 Identidad individual de los usuarios.

Todos los usuarios que participan en la *PKI* de *ANF AC*, son personas jurídicas legalmente constituidas o personas físicas, mayores de edad y plenamente capacitadas para asumir las obligaciones y responsabilidades que son inherentes a la posesión y uso de un certificado de *ANF AC*.

Se hace constar que los certificados emitidos por esta Autoridad de Certificación que tengan como titulares a personas jurídicas, contendrán además la identidad de una persona física que será la que esta en posesión del certificado y en disposición de poder utilizarlo.

7.2.j.5 Identidad de los representantes.

Debe de tratarse de personas físicas. Estas personas tienen que ser mayores de edad y plenamente capacitadas para poder asumir las obligaciones y responsabilidades derivadas de la representación que ostentan.

7.2.j.6 Procedimientos de resolución de disputas de nombres, denominaciones comerciales y marcas.

- Nombres

Cualquier disputa concerniente a la propiedad de nombres, es resuelta bajo criterio de la *ARR*, en caso de que el nombre ya figurará inscrito en *ANF AC*, prevalecerá el que primero figure registrado.

No obstante, *ANF AC* se reserva el derecho a revocar un certificado en caso de que sobre el mismo se haya establecido una disputa.

- Denominaciones comerciales y marcas

Caso de inclusión de marcas o denominaciones comerciales en el certificado, esta siempre se realizará a petición del titular o del representante del titular del certificado y bajo su exclusiva responsabilidad.

Caso de plantearse una disputa respecto a la propiedad de una denominación comercial o de una marca, siempre prevalecerá la de aquel que acredite ostentar su propiedad en el territorio español.
No obstante *ANF AC* se reserva el derecho a revocar un certificado en caso de que sobre el mismo se haya establecido una disputa.

7.2.k Método de prueba de posesión de la clave privada.

El método utilizado para garantizar que la clave privada esta en posesión del suscriptor es PKCS#10. El certificado de petición que contiene la clave pública que esta asociada a la privada, es cifrado con la clave privada. La capacidad de descifrar el fichero con la clave pública, acredita que el usuario esta en posesión de la privada que utilizó para cifrar y que ambas están asociadas.

7.2.l Autentificación de la identidad de una persona jurídica.

Cada Política de Certificación establece el procedimiento a seguir.

7.2.m Autentificación de la identidad de una persona física.

Cada Política de Certificación establece el procedimiento a seguir.

7.2.n Autentificación de la identidad de los representantes.

Cada Política de Certificación establece el procedimiento a seguir.

7.2.o Renovación rutinaria de un certificado.

Cada Política de Certificación establece el procedimiento a seguir.

7.2.p Renovación de un certificado después de una revocación.

Esta autoridad de certificación no permite la renovación de certificados revocados.

7.2.q Renovación de un certificado suspendido.

Esta autoridad de certificación no permite la suspensión de certificados.

7.2.r Solicitud de revocación o suspensión.

El método de identificación y autentificación para solicitar una revocación se establece en cada una de las modalidades contempladas en el apartado "Procedimiento de revocación de certificados".

Esta autoridad de certificación no permite la suspensión de certificados.

7.2.s Solicitud, denegación, emisión y aceptación de los Certificados.

7.2.s.1 Solicitud.

Este apartado se desarrolla de manera específica para cada tipo de certificado a través de su respectiva Política de Certificación.

7.2.s.2 Denegación.

Un sistema *PKI* se desarrolla en un marco de confianza mutua y en una relación de buena fe. Aquellas personas que mantengan o hayan mantenido directamente algún tipo de conflicto de intereses con esta entidad prestadora de servicios de certificación o con los miembros de su Junta Rectora, no pueden tramitar solicitud de emisión de certificados, ni instar a terceros a que lo realicen. Tampoco pueden realizar solicitudes de certificados personas pertenecientes o dependientes de entidades que son competencia de *ANF AC* .

ANF AC se reserva el derecho de denegar la emisión o renovación de certificados libremente y cuando lo estime oportuno.

7.2.s.3 Emisión.

Periódicamente y de acuerdo con las necesidades de servicio, dos responsables de *ANF AC* se personan en las instalaciones donde se encuentra el ordenador que contiene las Claves Privadas de *ANF AC* y que permite la emisión de los certificados de entidad final.

El procedimiento de emisión cuenta con un protocolo de obligado cumplimiento, y esta configurado de tal forma, que garantiza la trazabilidad de las actuaciones realizadas en cada momento.

7.2.s.4 Publicación.

Los certificados emitidos pasan a publicarse en el repositorio público del servidor del *PSC*.

7.2.s.5 Aceptación.

El mecanismo que determina el procedimiento a realizar es la Política de Certificación aplicable a cada certificado.

7.2.s Revocación de certificados de usuario final.

7.2.s .1 Procedimiento.

- **Presencial:**

Personándose en las oficinas de *ANF AC* cuya dirección consta en este documento o en cualquiera de oficinas de las Autoridades de Registro cuya lista figura en la URL:

https://www.anf.es/AR/

La persona física titular del certificado deberá acreditar su identidad mediante célula de identidad, pasaporte u otros medios admitidos en Derecho. En cualquier caso deberá presentar documentos originales.

En el caso de certificados expedidos a personas jurídicas, el solicitante deberá acreditar su identidad como queda reseñado en el anterior supuesto de "personas físicas" y además, deberá acreditar su facultad como representante legal , mediante poder notarial original o documento legal suficiente.

- **Telemáticamente:**

Mediante conexión telemática al Registro General, de acuerdo con el procedimiento establecido en la sección *"Accesibilidad –Usuarios de ANF AC -"* de esta DPC de *ANF AC* .

https://www.anf.es/AC/Revocados

- **Mediante correo tradicional:**

Enviando el formulario debidamente cumplimentado a las oficinas de *ANF AC* cuya dirección consta en este documento, firmando y reseñando en el mismo nombre de usuario, contraseña e identificador del certificado.

- **Mediante correo electrónico:**

Enviando un correo firmado electrónicamente. La firma deberá estar vinculada a un certificado emitido por *ANF AC* , o por alguna otra entidad de certificación oficialmente acreditada.

7.2.s.2 Método de comprobación.

El método de comprobación de la veracidad de las solicitudes, salvo las solicitudes de tramitación telemática cuyo método de verificación se realiza de forma automática e inmediata por coherencia de datos, se realiza valorando la correspondencia de los datos aportados por el solicitante y los existentes en los archivos de *ANF AC* , esta valoración se lleva a cabo por personal del área jurídica de *ANF AC* .

7.2.s.3 Efectos.

ANF AC no permite la suspensión temporal de certificados. La extinción de la vigencia del certificado electrónico revocado tiene efectos desde que la indicación de dicha extinción se incluya en el Registro General de *ANF AC*.

Las revocaciones son definitivas. Suponen la pérdida de eficacia de los certificados e impide al usuario el uso legítimo del mismo.

La revocación tiene efectos inmediatos en los certificados emitidos bajo la jerarquía de ANF ROOT CA, imposibilitando que el Dispositivo homologado de creación de firma electrónica pueda procesar su aplicación.

La referencia de todo certificado revocado es incluida en la Base de Datos del Registro General, y se expide simultáneamente una nueva CRL que lo incluye. Esta información tiene como efecto a terceros que lo consulten que el certificado ha sido revocado.

7.2.s.4 Ordenantes y causas de revocación

Tiene la capacidad de revocar los certificados el usuario, la persona que lo representa, la propia *ARR* que tramitó su identificación o este *PSC*. Cuando la revocación no sea solicitada por el usuario, *ANF AC* le notificará este hecho mediante correo electrónico remitido a la dirección que hizo constar el usuario en su solicitud de certificado, siempre que sea posible de manera previa a la revocación, o simultáneamente a que se produzca la misma. Este correo esta firmado electrónicamente.

Se procederá a la revocación del certificado a petición del usuario, la persona a la que representa, *ANF AC* o *ARR* por incumplimiento de las obligaciones impuestas en esta *DPC*, sus ANEXOS, Políticas de Certificación o en cualquiera de los supuestos que establece la legislación vigente.

En cualquier caso sí:

a. Ha existido pérdida, robo, modificación, divulgación no autorizada u otro compromiso de la clave privada asociada al certificado del usuario, o al del certificado que AC empleo para su emisión.
b. Se conoce o se tienen motivos para creer razonablemente que uno de los hechos representados en el certificado es falso.
c. Se conoce que alguno de los requisitos de emisión del certificado no fue cumplido.
d. El sistema de certificación se vio comprometido de modo tal que afecta a la fiabilidad del certificado.
e. Cese en la actividad del *PSC*, salvo que los certificados sean transferidos a otro prestador de servicios de certificación.

f. Cuando el certificado ha sido emitido en fecha posterior a que la clave privada de la *ANF AC* se haya visto comprometida y por tanto revocada.

g. El mal uso deliberado de claves y certificados, o falta de observación de los requerimientos operacionales del acuerdo de suscripción.

h. La negligente actuación del usuario en el ámbito de esta *PKI*, aunque se haya producido con otro certificado distinto al que se va a revocar.

i. Resolución judicial o administrativa que lo ordene.

j. Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

k. Si se produce la revocación del certificado que la CA empleo para la emisión.

l. Por la pérdida de vigencia de los algoritmos de firma o de hashing al ser calificados como “no seguros”.

m. Por la pérdida de vigencia de la longitud de clave, al ser calificada como “no segura” o “no autorizada”.

Si la solicitud de revocación es a instancias del propio titular o de su representante legal, deberá, tanto si se realiza en papel o en formato electrónico, contener la información que se especifica en el “Formulario de Solicitud de Revocación” incluido en cada Política de Certificación a la que se somete el certificado en cuestión.

7.2.s .5 Acreditaciones.

Independientemente del procedimiento seguido para efectuar la revocación del certificado por parte del Usuario o persona a la que representa, éstos pueden requerir de *ANF AC* que le sea expedida una acreditación del

estado de revocación en que se encuentra su certificado. Esta acreditación esta fechada y es firmada por *ANF AC* .

7.2.t Caducidad y renovación.

Cada Política de Certificación establece el procedimiento a seguir.

7.2.u Atributos.

Las especificadas en la Política de Certificación correspondientes al certificado emitido.

7.2.v Limitaciones de uso.

Las especificadas en la Política de Certificación correspondientes al certificado emitido.

7.2.w Condiciones de uso.

Para poder utilizar los certificados expedidos por *ANF AC* se requiere:

a) Que el certificado esté activado.
b) Que el contenedor de datos de creación de firma esté activado.
c) Utilizar un contenedor de datos de creación de firma homologado por *ANF AC* .

7.2.x Tasas de solicitud, activación, emisión y renovación.

Este apartado se desarrolla de manera específica para cada tipo de certificado a través de su respectiva *CP*.

7.2.y Registro General.

Toda la información y documentación relativa a los certificados emitidos por este *PSC*, así como los propios certificados y sus circunstancias históricas, especialmente incidencias de renovación y revocación, son conservadas y accesibles al menos por un periodo mínimo de quince años.

7.2.y.a Contenido.

a) Documental digitalizado:

- Documentación original relativa al proceso de identificación y autenticación que acredita la identidad de los usuarios de *ANF AC* .
- Documentación o informes realizados por el Departamento Jurídico de *ANF AC* o por la Autoridad de Registro.
- Histórico de Declaraciones de las Prácticas de Certificación, Políticas de Certificación y de Firma, y Anexos,.
- En general, escritos y documentos relacionados con los usuarios de *ANF AC* y sus certificados.

b) Datos informatizados.

ANF AC dispone de los siguientes servicios:

World Wide Web.

- *Con acceso a base de datos*:

  Identificador del certificado, fecha de emisión, fecha de caducidad, fecha de renovación, fecha de activación, revocación (fecha y causa), atributos, importe límite de firma electrónica, estado (activado, caducado, revocado), Nombre completo del usuario y seudónimo. Así mismo, registrará la dirección de correo electrónico, célula de identidad, dirección personal, población, provincia, país, teléfono y cuantos datos consten caso de tratarse de un certificado de entidad, o el usuario actúe en representación de terceras personas físicas o jurídicas. Acceso restringido a personas autorizadas por el titular del certificado.

  - *Con acceso a repositorio*. Copia del certificado emitido. Acceso restringido a personas autorizadas por el titular del certificado.

Servicio SOAP.

Que permite la actualización incremental telemática de la lista de certificados revocados.

Servicio OCSP.

Que tiene acceso a la lista de los certificados emitidos por *ANF AC* y permite determinar el estado de vigencia en que se encuentran. Con el fin de garantizar alta disponibilidad del servicio, la consulta se realiza sobre una red distribuida de servidores.

El servicio ha sido desarrollado siguiendo las recomendaciones de la norma:

[RFC2560] Internet X.509 PKI Online Certificate Status Protocol (OCSP).

Acceso restringido a entidades autorizadas.

CRL.

"Lista de Certificados Revocados". Se mantiene un histórico de todas las *CRL's* que *ANF AC* ha emitido.

El servicio ha sido desarrollado siguiendo las recomendaciones de la norma: [RFC-5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile .

7.2.y.b Accesibilidad.

Se permite el acceso al Registro General en todos los supuestos que contempla la legislación vigente sobre firma electrónica. No obstante la utilización de alguna de las modalidades de servicio de consulta están sometidas a acuerdo previo.

Usuarios de ANF AC .

Pueden acceder de forma telemática y en tiempo real, al contenido informatizado completo de sus respectivos datos a través del servicio WWW. El Usuario tiene la posibilidad de configurar el proceso que controla el acceso a esta información en base a las siguientes posibilidades:

a) Exclusivamente mediante Token homologado.
b) Habilitando el sistema de nombre de usuario y contraseña.

Así mismo pueden utilizar el servicio OCSP para obtener una verificación firmada por este PSC, que certifique el estado vigencia de su certificado. Este proceso deberá ser realizado empleando los dispositivos homologados por *ANF AC* .

El contenido documental original puede ser accesible concertando visita personal con la Oficina de Atención al Cliente. El usuario deberá acreditar de forma suficiente su identidad en el momento de la personación en las oficinas centrales de *ANF AC* . Los usuarios podrán solicitar por escrito, acreditando su identidad de forma suficiente, copia firmada por *ANF AC* de la documentación relativa al proceso de identificación y autenticación, así como de los escritos intercambiados con el *PSC*, corriendo a su cargo los gastos de confección y envío, el cual se realizará contra reembolso y certificado con acuse de recibo.

Terceros de confianza.

Las consultas de terceros se realizará por WWW y determinando de forma concreta identificador del certificado o nombre de usuario, no son permitidas consultas por aproximación. Pueden acceder de forma telemática y en tiempo real, al siguiente contenido:

Identificador del certificado, fecha de emisión, fecha de caducidad, fecha de renovación, fecha de activación, fecha de revocación, estado (activado, caducado, revocado).

Personal autorizado de *ANF AC* y *ARR*

Pueden acceder de forma telemática y en tiempo real, al contenido del Registro General y efectuar labores de mantenimiento dentro de las funciones que le son encomendadas. El control de acceso se realizará exclusivamente mediante token criptográfico que contienen los certificados digitales personales.

Otros procedimientos de acceso

Mediante acuerdo específico con *ANF AC* se podrán acceder a los restantes servicios e incluso, la implantación de servidores con dedicación exclusiva.

7.2.y.c Tasas de acceso a los certificados, e información de su estado de activación, revocación.

El acceso a la información mediante consulta World Wide Web y CRL's es libre y gratuita, y por tanto, no se aplicará ninguna tarifa. Cualquier otra modalidad de consulta se regulará mediante acuerdo específico.

7.2.y.d Contraseñas de Identificación reconocidas.

- Cada operador frente al sistema informático cuenta con sus propias claves de acceso: nombre de usuario y contraseña.
- Cada certificado cuenta con un Localizador AR que identifica al suscriptor en el Registro General.
- Cada certificado cuenta con un número de serie único y exclusivo que lo identifica en el Registro General.
- Cada certificado integra la clave pública que esta asociada matemáticamente con la clave privada en poder del usuario. Una copia del certificado se encuentra en el Registro General. Un mensaje cifrado con la clave privada permite identificar al usuario en el Registro General.
- El nombre y apellidos de cada Usuario junto con su número de: Documento Nacional de Identidad o Pasaporte o tarjeta de residencia, es un código de identificación único y exclusivo que lo identifica en el Registro General.
- El conjunto de respuestas correctas a las preguntas que configuró el usuario en su momento, es una clave que permite modificar la contraseña originalmente establecida por el usuario.

Configuración personalizada del acceso al Registro General:

- La accesibilidad al sistema mediante claves de identificación por parte de los Usuarios, viene determinada por el estado de activación o desactivación en que cada operador lo configura.
- Si está activado, el usuario puede acceder al Registro General, visualizar completamente sus datos personales e, incluso, efectuar las labores de mantenimiento, utilizando estas Claves que en BB.DD. se encuentran cifradas y requieren, por parte del usuario, una periódica actualización. En ningún caso puede modificar datos que afecten a la propia integridad o coherencia de los reseñados en el certificado.
- Si está desactivado, podrá utilizar estas claves para acceder al Registro General con la única posibilidad de revocar su certificado.
- En cualquiera de los supuestos anteriores, activado o desactivado el sistema de contraseñas, la utilización del identificador del certificado activado y vigente en el sistema de consultas del Registro General, habilita al solicitante para obtener una copia del certificado en cuestión.

Sistema de Preguntas y Respuestas:

En caso de olvido de la contraseña, el sistema informático tiene la capacidad de permitir al operador actualizar las claves de identificación.

Procedimiento telemático:

- Debe de introducir su nombre de usuario o número de serie del certificado.
- El sistema le efectúa las preguntas que en su momento configuró, las cuales deberá responder correctamente.

Modificación:

El usuario mediante su Token o utilizando nombre de usuario y contraseña (si está activada esta modalidad), puede modificar cuando lo desee los datos relativos a las claves de identificación o reconfigurar el sistema de claves de identificación (activarlo o desactivarlo).

Administración:

Administración de los registros.

- El Usuario de *ANF AC* o la persona física o jurídica a la que representa, tienen la capacidad de revocar su certificado siempre que lo deseen.
- El resto de operaciones de administración están reservadas a personal autorizado por *ANF AC* o las *ARR*.

Expedición de acreditaciones.

- Sobre ficheros firmados por usuarios, *ANF AC* expide a cualquier persona o entidad que se lo solicite, un informe que determine sí:

1) La firma digital corresponde al documento al que se la vincula.

Constatando:

a) la integridad cierta del documento,

b) la identidad del firmante,

c) el tipo de certificado al que se vincula la clave privada utilizada y,

d) atributos y limitaciones de uso.

2) El informe es fechado y firmado por *ANF AC* . El soporte en el que se emite el informe es electrónico.

Esta labor realizada por la AC es con cargo al solicitante.

7.2.z Mantenimiento de los datos.

ANF AC mantiene los datos y documentos relativos a la emisión de certificados, evolución e incidencias, por un plazo mínimo de 15 años contados desde el momento de su expedición, sin perjuicio del derecho de cancelación sobre aquellos datos de carácter personal que establezca la legislación vigente.

En cuanto al contenido de las Listas de Revocación, los certificados revocados podrán ser retirados de la *CRL* transcurridos tres meses después de haberse producido su caducidad. No obstante, *ANF AC* mantiene de forma permanente y accesible al público, un histórico de todas las *CRL's* que ha publicado.

7.2.za Frecuencia de la emisión de CRL's.

ANF AC publica una nueva *CRL* en su repositorio dentro del plazo máximo establecido en el campo "Next Update" (próxima actualización). *ANF AC* mantiene un histórico de todas las CRL emitidas. URL:

http://www.anf.es/AC/RC/index.html

En cuanto al campo "Next Update" (próxima actualización), se hace constar que la norma de referencia RFC-3280 v.1 no establecía como obligatorio el citado valor, pero la versión 2 si que lo requiere. Con el fin de garantizar la interoperabilidad con otros sistemas PKI se ha procedido a su inclusión. *ANF AC* informa que la fecha que se reseña en el citado campo, indica exclusivamente la fecha límite en la que se publicará una nueva CRL. EN NINGUN CASO presupone que NO SE VAYA a publicar una nueva actualización hasta ese momento.

7.2.zb Requisitos de comprobación de CRL's.

Los terceros de confianza deben de comprobar el estado de validez del certificado empleando los dispositivos de verificación homologados por *ANF AC*.

Caso de que la comprobación se realice consultando las listas de revocación CRL, y se efectúe en fecha posterior a la fecha de caducidad del certificado, se deberá consultar la CRL cuya fecha de emisión fue inmediatamente posterior al momento de producirse la caducidad del certificado.

7.2.zc Difusión Certificados de Usuarios.

ANF AC facilita copia de los Certificados de forma telemática. Los interesados pueden acceder al Registro General utilizando el número de serie de certificado en cuestión.

7.2.zd Cifrado de Datos.

El uso de Certificados de Cifrado de *ANF AC* se realizará bajo la exclusiva responsabilidad del usuario.

Se hace constar que algunos países prohíben o condicionan su uso, el suscriptor del certificado esta obligado a informarse en cada caso y adecuar su empleo a la legislación correspondiente.

8. Autoridad de Registro.

Para llevar a cabo la Prestación del Servicio de Certificación, *ANF AC* podrá realizarlo de forma autónoma o utilizando entidades colaboradoras que según características reciben el nombre de:

Autoridades de Registro Reconocidas, *ARR*.
Autoridades de Registro Colaboradoras.

Son Autoridades de Registro Colaboradoras, todas aquellos entidades que la legislación vigente les otorga la capacidad legal para llevar a cabo procesos de identificación, pese a no haber suscrito un acuerdo con este PSC. P.e. *Notarios*.

ANF AC dota a sus ARR de un dispositivo específico denominado AR Manager. Este instrumento esta configurado para que la *ARR* realice sus funciones de forma adecuada a los procesos establecidos por esta entidad prestadora de servicios de certificación.

Las funciones a realizar por las *ARR* pueden quedar ampliadas en cada Política de Certificación asociada a los certificados emitidos por este *PSC*. De forma general, y siempre en concordancia con lo especificado en cada *CP*, cabe enumerar las siguientes responsabilidades:

- Llevar a cabo la identificación y autentificación de los solicitantes de certificados de acuerdo con las estipulaciones reseñadas en las Políticas de Certificación asociadas al certificado solicitado. Así mismo y en caso de certificados de “Personas Jurídicas” le corresponde comprobar la identidad y autorización de la persona física que representa al solicitante.

- Verificar que el solicitante esta en plenas facultades y realiza el tramite sin mediar coacción. Deberá rechazar la tramitación si sospecha que la petición se efectúa bajo coacción, o en cualquier caso presuma que el procedimiento de solicitud no se ejercita bajo el principio del libre consentimiento.

- Informar al solicitante sobre sus Derechos y Obligaciones.

- Efectuar una estimación sobre:
  - La capacidad del solicitante para ostentar el certificado solicitado.
  - La adecuación de la clase de certificado solicitado a las características del solicitante.
  - Determinar la suficiencia y validez de las acreditaciones que acompaña a la solicitud y rechazar en caso de duda su tramitación.
  - En general, aceptar o denegar la tramitación de solicitudes de certificados. Las denegaciones deberán estar fundamentadas sobre bases objetivas y justificadas.

- Tramitar toda la documentación original presentada por el solicitante, tras obtener de la misma una copia (*siempre que sea posible en formato electrónico, utilizando en el proceso de digitalización el dispositivo AR Manager de ANF AC*), que compulsará firmándolas y numerándolas. En base a los datos acreditados proceder a:
  - Utilizando el dispositivo AR Manager deberá cumplimentar los formularios de solicitud y el contrato de prestación de servicios de certificación.
  - Imprimir los referidos documentos, los cuales serán firmados de forma manuscrita por el operador de la Autoridad de Registro que realiza el trámite y el usuario solicitante.
  - Remitir a *ANF AC* toda la documentación correspondiente a la solicitud tramitada.
  - En generar el acta de identificación y las claves de activación, nombre de usuario y contraseña (*ver características en Seguridad Criptográfica*).

- Una vez formalizados los documentos, se debe hacer entrega al solicitante:
  - Dispositivo de Generación de Datos de Creación de Firma.
  - Dispositivo de Creación de Firma Electrónica.
  - Dispositivo de Verificación

- Acta de Identificación que le permite generar su "certificado petición" y las claves de activación del acta.

Así mismo deberá requerir, previa a la formalización de la solicitud de emisión del certificado, que efectúe una lectura de sus Derechos y Obligaciones, informándole sobre las dudas que al respecto pueda tener. No se puede formalizar la solicitud de emisión del certificado hasta que el solicitante considere que tiene una compresión plena de los textos.

En cualquier caso, si el operador de la *ARR* estima que las consultas realizadas por el solicitante se encuentran fuera del ámbito de sus conocimientos u obligaciones, o bien, no logra resolver las dudas que le plantean, instruirá al solicitante para que contacte con la Oficina de Atención al Cliente de *ANF AC* y que sea personal especializado de ese departamento el que atienda y facilite gratuitamente el asesoramiento requerido.

La *ARR* asume la obligación de revocar los certificados por él tramitados o denegar una emisión de certificado en tramite cuando:

- Tenga conocimiento que las circunstancias del titular o del representante, en su caso, han cambiado.
- Tenga conocimiento de que se ha producido un quebranto que afecte a la seguridad de los datos de creación de firma.
- En cualquier supuesto en el que considere que su vigencia puede afectar negativamente a la confiabilidad de la *PKI* de *ANF AC*, su uso no este enmarcado en la buena fe, se utilice en perjuicio de terceros o en operaciones ilegales.

Los criterios de valoración que seguirá la *ARR* sobre la documentación aportada por el solicitante para acreditar identidad u otros datos a incluir en el certificado, serán los normalmente aceptados en Derecho. La Autoridad de Registro Reconocida siempre exigirá la presencia física del solicitante y siempre, la presentación de documentación original.

Las *ARR* podrán valerse de los medios que consideren necesarios para comprobar la veracidad de los datos y documentos aportados, incluso requerir al solicitante acreditación o información complementaria.

Todos los trámites realizados por las *ARR* son firmados electrónicamente por los operadores que los realizan, asumiendo así su plena responsabilidad en el proceso.

Las *ARR* cuentan con la autorización de cobrar las tasas de identificación, solicitud, activación e inclusión de atributos del certificado solicitado.

La valoración final de la suficiencia o no de la comprobación realizada por la *ARR*, así como de los documentos aportados siempre correrá a cargo de personal perteneciente a *ANF AC* .

9. Firma Electrónica y Sellos Digitales de Tiempo

Firma Electrónica

En todos los posibles aspectos, según lo especificado en la Política de Firma Electrónica.

OID : 1.3.6.1.4.1.18332.27

Sellos Digitales de Tiempo

En todos los posibles aspectos, según lo especificado en CPS de Autoridad de Sellado de Tiempo. **OID** : 1.3.6.1.4.1.18332.5

10. Obligaciones y Responsabilidades.

10.1 ANF AC .

10.1.1 Generales.

Se responsabiliza en cumplir con todas las obligaciones exigibles a los prestadores de servicios de certificación de acuerdo con la legislación vigente. Así como todas las derivadas del presente Documento, sus Anexos y Políticas de Certificación. La siguiente relación es meramente enunciativa y no limitativa.

Se compromete a:

- Proteger las Claves Privadas contra el peligro de usurpación.
- Emitir certificados en conformidad con las Políticas de Certificación que le sean aplicables.
- Emitir certificados de acuerdo con los requerimientos expresados en la solicitud, siempre que estos requerimientos sean compatibles con los términos expresados en esta *DPC*, sus Anexos y Políticas de Certificación.
- Conservar registrada toda la información y documentación relativa a un certificado emitido por *ANF AC* por un plazo de quince años a contar desde la fecha de caducidad del mismo, de manera que puedan verificarse las firmas efectuadas con el mismo.

10.1.2 Del repositorio.

- Mantener accesible vía Web para toda la comunidad que participa en esta PKI un repositorio con el conjunto de certificados emitidos en formato x.509.v3, con información actualizada y detallada sobre su estado: vigencia o revocación.
- Mantener accesible para el público en general el repositorio de sellos de tiempo.
- Mantener accesible para el público en general el repositorio de CRL.
- Mantener accesible para el público en general todos los documentos publicados por este *PSC*, independientemente de que se trate de versiones

no vigentes. En especial, se mantendrán todas las *DPC* publicadas y su respectiva addenda.

10.1.3 Limitaciones de las responsabilidades.

ANF AC no responderá de otros daños y perjuicios que los expresamente reseñados en la Ley de Firma Electrónica vigente.

El límite de responsabilidad en caso de pérdidas por transacciones, este PSC limita su responsabilidad exclusivamente a los certificados que emite bajo la calificación de reconocidos, y sobre ellos establece en cada certificado:

- Limitación de uso
- Limite monetario del valor de las transacciones, que queda reseñado en el propio certificado. Concretamente en la extensión "QCStatements" mediante el OID 1.3.6.1. 5.5.7.1.3 de acuerdo con la norma RFC 3739. La información queda reseñada de acuerdo con lo establecido en la norma TS 101 862 – 4.2.2 de la ETSI (European Telecommunications Standards Institute).

10.1.4 Deslinde de responsabilidades y limitaciones de pérdidas.

En ningún caso responderá de daños o perjuicios comerciales, profesionales o empresariales, salvo hayan sido expresamente aceptadas previamente por *ANF AC*.

ANF AC , salvo pacto expreso que regule algún tipo de penalización, no asume ninguna responsabilidad por la interrupción de los servicios de firma electrónica, independientemente de la causa que los ocasionen.

10.1.5 Ubicación segura luego de haberse producido accidentes o algún tipo de daño.

En el caso de que se deba establecer un sitio de procesamiento alternativo por la existencia de daños, el nuevo sitio tendrá, como mínimo, el mismo nivel de seguridad física y lógica que el sitio de procesamiento original. La nueva ubicación se hará de forma diligente y en el menor plazo de tiempo posible. El Plan de Reanudación de las Operaciones Comerciales de *ANF AC* , se encuentra

disponible para todo el que justifique la necesidad de conocerlo, en la Oficina de Atención al Cliente.

10.1.6 En caso de que los recursos, el software y/o los datos informáticos estén gravemente dañados.

En el caso de que se dañen gravemente los recursos, el software y/o los datos informáticos, se detendrá el funcionamiento de la AC y el sistema será restablecido una vez que se hayan incorporado nuevos componentes de eficiencia comprobable. Simultáneamente, se llevará a cabo una investigación para identificar la causa de los daños y se evaluará la integridad de la *PKI*. Se notificará a los Usuarios y a la Junta Rectora de la PKI acerca de los daños producidos.

10.1.7 En caso de que la clave de la entidad pueda ser usurpada.

Si la Clave Privada de la AC es usurpada, o está expuesta a dicho riesgo, se revocará inmediatamente el Certificado correspondiente, se actualizará y publicará la CRL, se detendrá el funcionamiento del sistema de la AC y se llevará a cabo un nuevo proceso de generación de claves de *ANF AC* . Además, se notificará a los Usuarios acerca de esta situación. Los Certificados emitidos antes de que se usurpara la Clave serán firmados nuevamente y aquellos que fueron emitidos luego de que se identificara la usurpación serán revocados. Se solicitará a los usuarios que generen un nuevo Par de Claves y que vuelvan a realizar el proceso de solicitud.

Se realizará un informe de lo acontecido, remitiéndolo a la Junta Rectora de la PKI.

ANF AC procederá al borrado de la clave comprometida de todos los dispositivos que la contienen, y en aquellos que la clave este integrada en una token criptográfico, se procederá a la destrucción física de la misma.

10.1.8 Cese de las actividades de la AC.

Las actividades de *ANF AC* sólo pueden ser suspendidas por su propia Junta Rectora. En el caso de que esto ocurra, *ANF AC* podrá ejercer su derecho de subrogación o bien, revocar todos los Certificados emitidos por *ANF AC* , suspendiendo de forma inmediata, a su vez, la emisión de nuevos Certificados.

ANF AC , se encargará de comunicar esta situación a todas los usuarios y a la Administración Pública, con la antelación que establezca la legislación vigente y en la forma que en ella se requiera, en cualquier caso con una antelación mínima de un mes.

10.1.9 Garantías Patrimoniales de ANF AC .

ANF AC garantiza su responsabilidad frente a sus usuarios y terceros de confianza de forma suficiente a lo establecido en la legislación vigente. A suscrito la correspondiente póliza de responsabilidad civil.

10.1.10 Subcontratación.

Aunque *ANF AC* puede optar por delegar una parte de sus roles y de sus respectivas funciones, siempre seguirá siendo responsable final d el desarrollo de sus servicios de certificación.

10.1.11 Exoneración de responsabilidad.

ANF AC no será en ningún caso responsable cuando se encuentra en alguna de las siguientes circunstancias:

- Estado de guerra, desastre natural o cualquier otra causa de fuerza mayor, incluida el funcionamiento defectuoso de los servicios de las redes telemáticas, fluido eléctrico o equipos informáticos.
- Acceso indebido por parte de terceros a los sistemas de certificación, ya sea mediante quebranto de las medidas de seguridad físicas (robo, hurto, actos de vandalismo o sabotaje), o de tipo informático (hasckers, crackers)
- Por el uso que se pueda realizar de los certificados, en especial por el contenido de los mensajes o documentos firmados o cifrados. Se hayan utilizado o no dispositivos homologados por este *PSC*.
- En relación a las omisiones, ocultación de datos realizada por el suscriptor o incluso, a la falta de veracidad de los mismos al haber empleado documentos o manifestaciones falsas, siempre y cuando la legislación vigente en materia de firma electrónica no requiera su verificación ante el ente emisor.

- Cuanto el tercero de confianza no cumpla sus obligaciones respecto al certificado que confía, de acuerdo con lo establecido en esta DPC.

10.2 Usuarios.

Se responsabiliza en cumplir todas las obligaciones derivadas del presente documento, sus anexos, Política de Firma Electrónica y Políticas de Certificación. Limitando, y adecuando el uso del certificado y de los sistemas de firma electrónica contemplados en el ámbito de esta PKI, a propósitos lícitos y acordes con una honesta y leal actuación con toda la comunidad: *ANF AC* , Autoridades de Registro Reconocidas, usuarios y terceros de confianza. La siguiente relación es meramente enunciativa y no limitativa.

El suscriptor se compromete a:

- Asegurarse de que toda la información contenida en el Certificado es cierta.
- Que en el momento de recibir su certificado electrónico, comprobar urgentemente la correspondencia del mismo con la petición formulada. Para ello, empleará la opción de comprobación de certificados que incluye el dispositivo de generación de datos de creación de firma. Caso de que la comprobación resulte negativa, comunicará el hecho de forma inmediata a *ANF AC* .
- Utilizar el certificado respetando las restricciones que le vienen impuestas según su Política de Certificación y la Política de Firma Electrónica.
- Caso de que el certificado reseñe “Declaración del Emisor, Atributos y Limitaciones de uso” , deberá atenerse a lo ahí indicado.
- Se obliga a custodiar, de forma diligente, el contenedor que contiene los datos de creación de firma y la clave secreta de activación, así como nombre de usuario y contraseña secreta de acceso al Registro General.
- Emplear exclusivamente dispositivos homologados por *ANF AC* , tanto para el almacenamiento de los datos de generación de firma, como para la creación de firmas electrónicas, como su posterior verificación.
- Mantener actualizados los dispositivos de firma electrónica homologados por *ANF AC* , siguiendo en su instalación y mantenimiento, las instrucciones que a tal efecto le facilite *ANF AC* .

- Previo a la creación de una firma electrónica empleando un dispositivo de firma homologado por *ANF AC* , el usuario se compromete a verificar los atributos de firma que serán incluidos la firma electrónica, y solo activará el proceso de firma si esta conforme con todos ellos.
- Aceptar todas las firmas electrónicas vinculadas al certificado del que es titular, siempre que hayan sido creadas empleando un certificado vigente.
  La imprescindible activación de los datos de creación de firma por parte del signatario mediante el empleo de su clave secreta, presupone: el consentimiento pleno de creación de la firma electrónica, y la aceptación de la Política de Firma Electrónica asociada a esa firma.
- A solicitar la revocación del Certificado cuando se vea comprometida la seguridad de los datos de creación de firma o la clave secreta de activación o sus datos personales hayan sufrido alguna modificación.
- En aquellos casos en los que el usuario o la persona jurídica a la que representa tenga contratados servicios de certificación personalizados. P.e. a modo meramente enunciativo que no limitativo cabe señalar:
  - Servicio de Notariado Electrónico en Exclusiva.
  - Servicio Mensajería Electrónica.
  - Servicio Facturación Electrónica...etc,

  el suscriptor en caso de revocación del Certificado, se obliga a cesar en su uso, siguiendo el procedimiento establecido en el momento de la contratación del servicio.
- Los usuarios garantizan que las denominaciones, nombre o dominios reseñados en el formulario de solicitud y en la contrato de prestación de servicios:
  - no infringe los derechos de terceros en ninguna jurisdicción con respecto a derechos de propiedad industrial y marca, que no emplearán el dominio y nombre distintivo para propósitos ilícitos; entre ellos, competencia desleal, suplantación, usurpación y actos de confusión en general.

  Los solicitantes y, en general, los usuarios de certificados, indemnizarán a *ANF AC* por los daños que le pueda causar en la realización de estas actividades.

- Suministrar a las *ARR* documentación original e información que consideren exacta y completa. Así como a notificar cualquier modificación que sobre la misma se produzca.
- Abonar las tasas de los servicios que le sean prestados por parte de la AC, o por parte de la *ARR*.
- No tramitar solicitud de certificado algún caso de haber mantenido algún tipo de conflicto de intereses con *ANF AC* o miembros de la Junta Rectora.
- La solicitud de certificado solo puede realizarse bajo el principio de la buena fe, y con el único interés de hacer uso del mismo para los fines que comúnmente son aceptados.

10.3 Terceros de confianza.

Tiene la consideración de receptor, el tercero de buena fe que confía en el fichero electrónico que está firmado digitalmente por un usuario de *ANF AC* y que, además de depositar la confianza en esa firma electrónica, cumpla con las siguientes obligaciones:

- Debe de verificar la firma utilizando un dispositivo de verificación de firma electrónica homologado por *ANF AC* .
- Comprobar el estado de vigencia del certificado utilizando uno de los medios autorizados por este *PSC*.
- El destinatario del documento o fichero electrónico firmado debe de actuar de forma diligente.
- Debe de valorar la adecuación del certificado asociado a la firma electrónica, de acuerdo con: el tipo de certificado, la declaración del emisor, las limitaciones de uso que en el mismo se reseñan, y las declaradas en esta *DPC* y la Política de Certificación a la que se somete..
- Debe de solicitar el asesoramiento de la “Oficina de Atención al Cliente” de *ANF AC* en caso de duda.

Los receptores que no cumplan los requisitos indicados, no podrán ser considerados de buena fe.

10.4 Autoridades de Registro.

10.4.1 Colaboradoras

Al no existir ningún tipo de vínculo contractual entre éstas y *ANF AC* , no existen otras obligaciones o derechos que los propios por los que se rige su actividad.

10.4.2 Reconocidas

10.4.2.a Generales.

Las *ARR* están obligadas a realizar todas sus operaciones en conformidad con lo establecido en esta *DPC* y la Política de Certificación aplicable en cada caso.

La siguiente relación es meramente enunciativa y no limitativa:

- Transcribir con exactitud en los formularios de solicitud del dispositivo AR Manager, la información recogida de los documentos originales aportados por los solicitantes.
- Admitir únicamente documentación original en el proceso de identificación, obteniendo copia de la documentación aportada por los usuarios. Documentación que será remitida a la autoridad de certificación para su guarda y custodia.
- No facilitar a terceros copia de la documentación obtenida de los solicitantes, ni información alguna de los mismos.
- Custodiar el dispositivo AR Manager, no permitiendo su uso o la revisión del mismo por terceros no autorizados. Y, en caso de pérdida, comunicarlo inmediatamente a *ANF AC* .
- Aplicar las tasas oficiales sin efectuar incremento, ni cargo alguno por ningún otro concepto que no sea los estipulados por *ANF AC* .
- En caso de cese en la actividad como *ARR*, deberá proceder a la devolución del dispositivo AR Manager, así como de cuanta documentación o material obre en su poder derivado de la actividad realizada como Autoridad de Registro Reconocida.
- Debe comunicar cualquier reclamación judicial o extrajudicial que se produzca en el ámbito de su actividad como *ARR*.

- En relación a la información contenida en el certificado o características personales que le capacitaron en su momento para obtener la acreditación como Autoridad de Registro Reconocida, debe de informar de cualquier cambio que se produzca en sus circunstancias personales..
- Debe proteger y custodiar personalmente las Claves Privadas de la *ARR* y la contraseña de activación, contra peligro de usurpación o uso indebido. Ante cualquier sospecha de quebranto de seguridad debe comunicarlo inmediatamente y proceder a su revocación.
- Ser diligente en la atención de los usuarios solicitantes. Facilitando, a ser posible, información de los documentos originales que les serán requeridos y evitando esperas innecesarias.
- No utilizar las copias que el solicitante acompañe a la documentación original. Cualquier copia en papel o digitalizada será obtenida directamente por la Autoridad de Registro.
- Comunicar de forma diligente a *ANF AC* la existencia de solicitudes de emisión de Certificados, en especial aquellas que ha rechazado.
- No mediar en la generación de los datos de creación de firma de los usuarios, ni permitir ser informado del PIN de activación elegido por el solicitante.
- Almacenar de forma segura y permanente, copia de la documentación aportada por el usuario para realizar su petición, así como de la documentación generada por el AR Manager, durante el proceso de petición, registro, o revocación.
- Colaborar con las auditorias dirigidas por *ANF AC* para validar la renovación de sus propias claves.
- Respetar la intimidad de los solicitantes y titulares de certificados.

10.4.2.b Deslinde de responsabilidades y limitaciones de pérdidas.

Las *ARR* no responderán de otros daños y perjuicios que los expresamente reseñados en la Ley de Firma Electrónica vigente. En ningún caso responderán de daños o perjuicios comerciales, profesionales o empresariales, salvo que exista contrato de prestación de servicios expreso

que hayan sido previamente aceptados por la Autoridad de Registro Reconocida y por *ANF AC* .

11. Responsabilidad Financiera.

11.1 Indemnización a las partes confiantes.

ANF AC de acuerdo con lo establecido en la vigente Ley, ha suscrito un seguro de responsabilidad civil para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que emita.

Los datos relativos a la póliza contratada constan publicados en la URL:

https://www.anf.es/AC/seguro/

11.2 Relaciones fiduciarias.

ANF AC no se desempeña como agente fiduciario ni representante en forma alguna de los usuarios, ni de los terceros de confianza, en los certificados que emite.

11.3 Procesos administrativos.

ANF AC garantiza la realización de auditorías de los procesos y procedimientos de forma regular.

12. Política de Confidencialidad.

12.1 Protección de Datos de Personales

ANF AC se compromete a no difundir o ceder a terceros, sin consentimiento expreso del interesado, ningún dato al que tenga acceso en razón de la prestación de sus servicios de certificación. Dichos datos son tratados, exclusivamente, para prestar los servicios requeridos.

ANF AC se compromete a proteger los datos recibidos por parte de los solicitantes de certificados o las Autoridades de Registro, poniendo las medidas de seguridad adecuadas.

No obstante, *ANF AC* se reserva el derecho a revelar a los empleados y consultores, externos o internos, los datos necesarios para realizar sus actividades como PSC. En este caso los empleados y/o consultores son informados sobre las obligaciones de confidencialidad recogidas en este epígrafe, debiendo suscribir los correspondientes compromisos de confidencialidad antes de acceder a los mismos.

Estas obligaciones no se aplican si la información calificada como "confidencial" es requerida por los Tribunales u órganos administrativos competentes o impuesta por una ley.

12.2 Tipos de información confidencial

Se declara expresamente como información confidencial y no podrá ser divulgada a terceros, excepto en los casos en que la ley exija lo contrario:

- La identidad de los titulares de certificados que han sido emitidos bajo un seudónimo.

- Cualquier información o dato, que habiendo sido aportado por el usuario a la autoridad de certificación o la autoridad de registro, no conste en el certificado digital.
- Toda información relativa a los parámetros de seguridad.
- Procedimientos de alta seguridad.
- Las claves privadas de *ANF AC* , de las Autoridades de Registro y de los usuarios.
- Cualquier otra información que *ANF AC* o la Junta Rectora de la PKI clasifique como “Confidencial”.

12.3 Envío a la autoridad judicial y/o policial

Como norma general ningún documento o registro perteneciente a *ANF AC* se envía a las autoridades judiciales o policiales, excepto cuando:

- El agente de la ley se identifica adecuadamente.
- Se proporcione una orden judicial debidamente redactada.
- La Autoridad de Certificación o de Registro tengan conocimiento que los certificados emitidos, o alguno de los instrumentos pertenecientes a esta PKI, están siendo utilizados para la comisión de un delito.

12.4 Divulgación a petición del propietario

El usuario titular podrá requerir a *ANF AC* la emisión de un informe de los datos que posee relativos a su persona. *ANF AC* facilitará presupuesto de la tasa correspondiente a ese servicio, y tras la aceptación, expedirá el mencionado informe.

12.5 Otras circunstancias de publicación de información

No esta permitida la divulgación de información bajo ninguna otra circunstancia de las reseñadas en los puntos expresados en este documento.

13. Oficina de Atención al Cliente.

ANF AC se compromete a tener plenamente operativo un servicio gratuito de atención de Usuarios y Receptores.

13.1 Cometido de la Oficina.

Este servicio atenderá cuantas consultas comerciales, jurídicas y técnicas estén relacionadas con:

- La actual legislación vigente sobre firma electrónica.
- Esta *DPC*, ANEXOS, Políticas de Certificación y documento de solicitud de certificados.
- Instalación y utilización de los dispositivos relacionados con la firma electrónica.
- Instalación y utilización del software homologado.
- Generación y uso de los contenedores homologados y, en general, todo lo relacionado con la prestación de servicios de certificación que esta AC realiza.
- Consultas generales sobre los conceptos básicos de Infraestructura de Clave Pública, certificados digitales y firma electrónica.

Así mismo, realizará en nombre del Usuario o de la persona a la que éste representa, las distintas operaciones que esta *DPC*, sus Anexos y Políticas de Certificación le encomienden.

13.2 Procedimiento de Consulta.

Las consultas se realizarán mediante correo electrónico dirigido a :

consultas@anf.es

en ellas se reseñará el identificador del usuario que consulta o, en caso de ser receptor, el identificador de la firma recibida.

Las consultas así realizadas son contestadas por este mismo medio a la dirección electrónica del remitente.

13.3 Procedimiento de Reclamación.

En caso de desear presentar una reclamación, esta entidad prestadora de servicios de certificación, cuenta con formularios al efecto URL:

https://www.anf.es/AC/reclamaciones/

O también se puede dirigirse personalmente ante la Oficinas de Atención al Cliente.

ANF AC contestará por escrito a la reclamación formulada en un tiempo no superior a 15 días hábiles. Caso de que la respuesta no sea satisfactoria, se seguirá con lo reseñado en el apartado “Procedimientos de resolución de disputas”, de este documento.

14. Interpretación y Ejecución.

14.1 Ley aplicable.

La legislación aplicable a este documento, y a las relaciones jurídicas subyacentes es la española.
Esta *DPC* debe interpretarse con arreglo a la legislación vigente, sus disposiciones de desarrollo y la legislación específica que afecta a sus servicios.

14.2 Conflicto de normas.

Cada certificado se emite bajo una *DPC* y una Política de Certificación, identificadas por un número de versión, de modo que, en cada caso, deberá acudirse a esa concreta versión, con independencia de posteriores versiones de tales documentos.

La *DPC* y las Políticas de Certificación se incorporarán por referencia a los certificados bajo las cuales se emiten tales certificados, a fin de que el receptor de los mismos disponga de elementos suficientes para valorar si decide confiar en los certificados y las firmas digitales vinculadas a los mismos.

14.3 Divisibilidad, supervivencia y notificaciones.

Cada cláusula de esta *DPC*, sus Anexos y Políticas de Certificación, es válida en sí misma y, en caso de anulación, no invalidará el resto. La cláusula inválida o incompleta podrá ser sustituida por otra equivalente y válida por acuerdo de las partes.

Las normas sobre obligaciones y responsabilidades, y todas aquéllas relacionadas a la confidencialidad y privacidad de los datos que han sido confiados a *ANF AC*, permanecerán en vigor tras la finalización de la vida de esta *DPC*.

Las notificaciones a *ANF AC* podrán realizarse mediante mensajes de correo electrónico firmados digitalmente, de acuerdo con las prescripciones de esta *DPC*, o por escrito.

Las comunicaciones electrónicas serán efectivas tras la recepción por parte del emisor del correspondiente acuse de recibo firmado digitalmente.

Las comunicaciones escritas deben ser enviadas por servicio certificado con acuse de recibo o equivalente.

14.4 Subrogación.

ANF AC , en caso de cese de su actividad, se reserva el derecho de transmitir en el futuro todos los sistemas de certificación a otro prestador de servicios de certificación. Se procederá a la extinción de la vigencia de los certificados emitidos, salvo que el suscriptor consienta expresamente la subrogación de la gestión de su certificado al nuevo prestador de servicios de certificación.

ANF AC comunicará, con una antelación mínima de tres meses, a los titulares de los certificados y a los solicitantes de los certificados de personas jurídicas, el cese de su actividad, informando sobre las características del prestador que se subroga la actividad, solicitando autorización expresa para mantener la vigencia de sus certificados con el nuevo gestor. Si transcurridos dos meses desde la comunicación no se ha recibido autorización expresa, se entenderá por denegada la autorización de subrogación y se procederá a la extinción de la vigencia del certificado.

ANF AC , remitirá, antes del cese de su actividad, a la Administración Pública competente, información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que se haga cargo de su custodia.

14.5 Administración de la DPC y Políticas de Certificación.

La propia evolución de los servicios de certificación de *ANF AC* , conlleva que esta *DPC*, sus Anexos y Políticas de Certificación estén sujetas a modificaciones. Se establece un

sistema de versiones numeradas para la correcta diferenciación de las sucesivas ediciones que de estos documentos se produzcan.

ANF AC se compromete a notificar a todos sus usuarios y Autoridades de Registro Reconocidas, con una antelación de 30 días a la entrada en vigor de las nuevas versiones, el texto integro de las mismas.

Toda necesidad de modificación debe estar justificada desde el punto de vista técnico, legal o comercial, debiendo, por lo tanto, estar avalada por la firma de los responsables de *ANF AC*.

Se deberán contemplar todas las implicaciones técnicas y legales de la nueva versión de especificaciones. Se establecerá un control de modificaciones para garantizar, en todo caso, que las especificaciones resultantes cumplen con los requisitos que se intentaban cumplir y que dieron pie al cambio.

14.6 Procedimientos de resolución de disputas.

14.6.a Procedimiento aplicable para la resolución extrajudicial de los conflictos.

ANF AC se somete voluntariamente para la solución de cualquier cuestión litigiosa que pudiera surgir por el ejercicio de su actividad, al arbitraje institucional del Tribunal Arbitral del Consejo Empresarial de la Distribución (TACED), al que se le encarga la designa del Árbitro – que será único – y la administración del arbitraje – que será de equidad – con arreglo a su Reglamento, obligándose desde ahora, al cumplimiento de la decisión arbitral.

Caso de que la alguna de las partes contrarias a *ANF AC* no acepte este procedimiento arbitral, se seguirá lo establecido en el apartado siguiente.

14.6.b Procedimiento judicial.

Todas las partes se someten expresamente a los Juzgados y Tribunales de la ciudad de Barcelona, con renuncia a su propio fuero si fuese otro.

15. Publicación y repositorios.

15.1 Publicación de información de la CA.

Es obligación de esta autoridad de certificación publicar información relativa a sus prácticas, sus certificados y el estado en que se encuentran dichos certificados. Todo el histórico de esta documentación deberá estar conservado y accesible al menos por un periodo mínimo de quince años.

Este documento y sus anexos son públicos y se encuentran disponibles en el sitio Web de la autoridad de certificación https://www.anf.es/AC/documentos/.

Las Políticas de Certificación son públicas y se encuentran disponibles en el sitio Web de la autoridad de certificación https://www.anf.es/AC/documentos/.

El certificado de la CA de *ANF AC* es público y se encuentra disponible en el sitio Web de la autoridad de certificación http://www.anf.es .

Los certificados emitidos por *ANF AC* son públicos y se encuentran disponibles en el sitio Web de la autoridad de certificación http://www.anf.es . Su consulta sobre base de datos, esta regulada en este documento, al igual que la obtención de una copia repositorio.

La lista de certificados revocados por *ANF AC* es pública y se encuentra disponible en el sitio Web de la autoridad de certificación http://www.anf.es . Su consulta sobre base de datos, esta regulada en este documento, al igual que la obtención de una copia en formato CRL v.2 del repositorio. Las distintas listas de CRL's que han sido publicadas por *ANF AC,* permanecen permanentemente disponibles al público, en ningún caso se procederá a su borrado o destrucción.

Todos los documentos se encuentran firmados electrónicamente por *ANF AC*. La integridad y autenticidad de los mismos debe de ser comprobada mediante dispositivo de verificación homologado por *ANF AC*, de libre distribución, puede ser descargado a través de la URL:

https://www.anf.es/AC/dispositivos/

15.2 Frecuencia de publicación.

La *DPC* y las Políticas de Certificación se publicarán en el momento de su creación.

Los certificados emitidos por la CA se publican de forma inmediata a su emisión.

El *PSC* crea, simultáneamente al acto de revocación del certificado, una nueva CRL que lo incluye.

Los Sellos de Tiempo se integran en el repositorio de *ANF AC* de forma simultánea a su creación.

15.3 Controles de acceso.

El acceso a lectura de la información del repositorio de *ANF AC* y de su Web es libre.

Solo *ANF AC* está autorizada a modificar, sustituir, añadir o eliminar información de su repositorio y sitio Web. *ANF AC* utiliza medios de control adecuados para restringir la capacidad de escritura o modificación de estos elementos.

15.4 Procedimiento de especificación de cambios.

Esta Declaración de Practicas de Certificación y las Políticas de Certificación pueden sufrir cambios en el transcurso del tiempo.

La entidad con atribuciones para analizar los cambios sobre esta *DPC* y las CP de *ANF AC* es la Junta Rectora de la PKI "*JRPKI*", cuyos datos constan en el "*Especificación del ente organizador".* La *JRPKI* determinará en cada caso, los elementos que le servirán de soporte para efectuar los análisis de los cambios propuestos, aunque deberá contar

siempre con un informe jurídico que establezca que estos cambios se adecuan a lo establecido en la legislación vigente.

La entidad con atribuciones para definir y aprobar sobre cualquier propuesta de modificación de esta *DPC* y las CP de *ANF AC* es la Junta Rectora de la PKI. Si el informe es negativo, no será posible realizar los cambios planteados.

Cuando se produzca un cambio en la *DPC* o en alguna de las CP de *ANF AC* se modificará el número de versión del documento afectado, incrementando en uno el número menor del valor de la versión existente (inmediatamente posterior al prefijo). Asimismo se podrá variar el número mayor de la versión (prefijo), si a juicio de la *JRPKI* los cambios efectuados son de tal importancia que recomienden realizar esa modificación. El nuevo prefijo es determinado por la propia *JRPKI*.

El mantenimiento y el control de la correcta aplicación de lo establecido en la Declaración de Prácticas de Certificación, sus Anexos y Políticas de Certificación, recaen sobre la Dirección Ejecutiva de *ANF AC*.

15.5 Procedimiento de Publicación y Notificación.

Cuando se produzca un cambio de versión, se comunicará a todos los usuarios de esta PKI y a las Autoridades de Registro mediante correo electrónico. Así mismo se publicará del repositorio de documentos de la Web de esta autoridad de certificación.

15.6 Procedimientos de aprobación de la DPC

La entidad con atribuciones para aprobar los cambios sobre esta *DPC* o en alguna de las CP de *ANF AC* es la Junta Rectora de la PKI. Cuyos datos constan en el apartado "*Especificación del ente organizador".*

La Junta Rectora de la PKI, notificará los cambios al equipo ejecutivo de *ANF AC* para que confeccionen una nueva *DPC* o CP según el caso. Proceda a su publicación,

notificación, y en caso de necesidad realizar las operaciones logísticas y operativas que adecuen la actividad de la autoridad de certificación a los nuevos requerimientos.