Servicio cualificado de conservación de firmas y sellos electrónicos cualificados (QEs)

Declaración de prácticas del servicio y Política de Conservación

Paseo de la Castellana,79 -28046- Madrid (España)

Telefono: 932 661 614 (Llamadas desde España)

Internacional +34 933 935 946

Web: www.anf.es

Nivel de Seguridad

Documento Público

Aviso Importante

Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (España)

Teléfono: 932 661 614 (llamadas desde España) Internacional (+34) 933 935 946

Web: www.anf.es

Control del documento

Nombre del documento e identificación

Nombre del documento	Servicio cualificado de conservación de firmas y sellos electrónicos cualificados (QEs). Declaración de prácticas del servicio y Política de Conservación		
Versión	1.5.		
OID	1.3.6.1.4.1.18332.61		
Fecha de aprobación	20/02/2025	**Fecha de publicación**	20/02/2025

Revisiones

Versión	Cambios	Aprobación	Publicación
1.5.	Corrección de referencia a la DPC. Actualización del certificado del servicio.	20/02/2025	20/02/2025
1.4.	Revisión anual, cambios de redacción menores.	14/03/2024	14/03/2024
1.3.	Revisión anual e inclusión del perfil de conservación, anteriormente reseñado en el documento 1.3.6.1.4.1.18332.61.10	26/02/2023	26/02/2023
1.2.	Revisión del perfil con cambio de WTS a WST	23/04/2021	23/04/2021
1.1.	Revisión anual	28/11/2020	28/11/2020
1.0.	Versión inicial. Creación del documento.	15/01/2020	15/01/2020

INDICE

1. Introducción

ANF Autoridad de Certificación [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 NIF G-63287510.

ANF AC utiliza OIDs según el estándar ITU-T Rec. X.660 y el estándar ISO/IEC 9834-1:2005 *(Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).* ANF AC 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-)*.

La Infraestructura de Clave Pública (PKI) de ANF AC ha sido diseñada y es gestionada en conformidad con el marco legal del Reglamento (UE) 910/214, y con la Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza de España. La PKI de ANF AC está en conformidad con las normas ETSI EN 319 401 *(General Policy Requirements for Trust Service Providers),* ETSI EN 319 411-1 (*Part 1: General Requirements*), ETSI EN 319 411-2 *(Part 2: Requirements for Trust Service Providers issuing EU Qualified Certificates)*, ETSI EN 319 412 *(Electronic Signatures and Infrastructures (ESI): Certificate Profiles)* y RFC 3739 (*Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*); ETSI EN 319 521 "*Policy and security requirements for Electronic Registered Delivery Service Providers*"; ETSI EN 319 522 "*Electronic Signatures and Infrastructures (ESI) Electronic Registered Delivery Services*"; ETSI TS 119 511 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques*"; ETSI TS 119 512 "*Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services*".

ANF AC, emplea las técnicas criptográficas indicadas en la norma TS 119 312 y la duración de la evidencia queda determinada por lo establecido en dicha norma. En procesos de 2FA (Doble Factor de Autenticación) se siguen las directrices del estándar PCI SSC v3.2 respecto al uso de la Autenticación Multi-Factor.

A efectos de esta política de certificación, ANF AC es Prestador del "Servicio Cualificado de Conservación de Firmas Electrónicas Cualificadas" y del "Servicio Cualificado de Conservación de Sellos Electrónicos Cualificados", previstos en los artículos 34 y 40 respectivamente, del Reglamento (UE) n° 910/2014[1].

Además, ANF AC presta servicio de Digitalización Certificada mediante la solución Legal Snap Scan® acreditada por la Agencia Estatal de Administración Tributaria, en conformidad con la Resolución de 24 de octubre de 2007 de la Agencia Estatal de Administración Tributaria (AEAT), correspondiente a software de digitalización

[1] Toda mención del presente documento al Reglamento 910/2014, incluye el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital

contemplado en la Orden EHA/962/2007, de 10 de abril de 2007. Para atender los requerimientos fiscales, la plataforma de conservación a largo plazo sometida a esta política de certificación incluye información relativa al contenido de los documentos en Metadatos y en base de datos.

El presente documento es la **Política del Servicio Cualificado de Conservación de Firmas Electrónicas Cualificadas y del Servicio Cualificado de Conservación de Sellos Electrónicos Cualificados** que ANF AC aplica en el desarrollo de su responsabilidad como Prestador Cualificado de Servicios de Confianza en cumplimiento del Reglamento eIDAS y la legislación nacional vigente.

La presente política es conforme a la norma del ETSI TS 102 573 "*Policy requirements for trust service providers signing and/or storing data objects*" y la RFC 3647 "*Certificate Policy and Certification Practices Framework*", define los requisitos de procedimiento y operacionales a los que está sujeto el uso del servicio, y define las directrices que ANF AC aplica para la prestación del perfil WST:

- Conservación y almacenamiento de firmas electrónicas cualificadas
- Conservación y almacenamiento de sellos electrónicos cualificados

Este documento es sólo uno de los diversos documentos que rigen la PKI de ANF AC, detalla y complementa lo definido en la Declaración de Prácticas de Certificación y su adenda. Esta política está subordinada a la Declaración de Prácticas de Certificación (DPC) de ANF AC. ANF AC tutela y supervisa que esta PC sea compatible y esté en coherencia con el resto de documentos que ha elaborado. Toda la documentación está a libre disposición de usuarios y terceros que confían en https://www.anf.es.

Esta política se publica en versión de idioma español e inglés, en caso de discrepancia, prevalece la versión de idioma español.

Esta Política asume que el lector conoce los conceptos de PKI, certificado, firma electrónica y almacenamiento y conservación a largo plazo; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.1. Descripción del servicio

Modalidad del servicio prestado, perfil WST:

- Conservación y almacenamiento de firmas electrónicas cualificadas
- Conservación y almacenamiento de sellos electrónicos cualificados.

1.1.1. Identificadores de cada modalidad de servicio

Con el objeto de identificar los servicios de conservación cualificada en sus diferentes modalidades, ANF AC les ha asignado los siguientes identificadores (OID) además de 0.4.0.19511.1.2. (Servicio cualificado que cumple con el Anexo A de ETSI TS 119 511):

Conservación y almacenamiento de firmas electrónicas cualificadas	1.3.6.1.4.1.18332.61.5
Conservación y almacenamiento de Sellos Electrónicos Cualificados	1.3.6.1.4.1.18332.61.6

El mismo perfil se aplicará durante todo el período de conservación.

El perfil no cambiará en el transcurso del tiempo, por lo que el perfil no incluye aspectos dinámicos fuera del perfil de conservación.

<table>
<tr><th colspan="4">ANF AC Servicio de conservación</th></tr>
<tr><td rowspan="4">Subject</td><td>CN = ANF AC Servicio de conservación</td><td>Serial number</td><td>033A3BA82311E8F0138BB695</td></tr>
<tr><td>OI = VATES-G63287510</td><td rowspan="2">Clave Pública</td><td rowspan="2">RSA (2048 Bits)</td></tr>
<tr><td>OU = Certificado Cualificado de Sello Electronico</td></tr>
<tr><td>O = ANF Autoridad de Certificacion</td><td rowspan="2">Algorítmo defirma</td><td rowspan="2">Sha256RSA</td></tr>
<tr><td>C = ES, L = BARCELONA, S = BARCELONA</td></tr>
<tr><td>Periodo de vigencia</td><td colspan="3">Válido desde el 05/02/2025 10:15:24 hasta el 30/01/2030 10:15:24</td></tr>
<tr><td>Fingerprint SHA-1</td><td colspan="3">1DC5D45005192E240E0B8D7D0B3C82500CCE39C4</td></tr>
<tr><td>Fingerprint SHA-256</td><td colspan="3">1849D7DAC70F7C1CAC460658B218E3818E6895B091E0E91A89272ABF78002E52</td></tr>
</table>

1.1.2. Evidencias electrónicas

Las evidencias electrónicas se generan incluyendo metadatos en la cabecera de los ficheros de datos, y firmando los datos transmitidos por el suscriptor, empleando en la elaboración un certificado de Sello Electrónico Cualificado de ANF AC.

Las evidencias electrónicas no contienen información explícita sobre el servicio de conservación o Política de Conservación aplicable, aunque sí incluye metadatos el servicio empleado en su autenticación y marca de tiempo correspondiente al momento en que fueron recibidos los datos.

ANF AC, dispone de la capacidad necesaria para elaborar como mínimo firmas/sellos electrónicos avanzados (requerimientos de Política Normalizados (N)), aunque la plataforma de conservación de largo plazo ha sido configurada con la capacidad de utilizar requerimientos de Política Extendidos (N+), empleando certificados cualificados, para poder, en su caso, elaborar firmas electrónicas cualificadas.

Con el fin de maximizar su interoperabilidad, se utilizan formatos de firmas AdES conformes a,

- **CAdES LT** *(ETSI EN 319 122)*
- **PAdES LT** (ETSI EN 319 142)
- **XAdES LT** (ETSI EN 319 132)

Se aplica los algoritmos, longitudes de clave y procedimientos establecidos en la Declaración de Prácticas de Certificación de ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1.

1.1.3. Certificación

ANF AC, en su calidad de Prestador Cualificado de Servicios de Confianza y emisor de los certificados de firma y sello electrónico cualificados, es el emisor de los certificados cualificados empleados por la plataforma de conservación y almacenamiento a largo plazo.

1.1.4. Validación

ANF AC, en su calidad de Prestador Cualificado de Servicios de Validación de Firmas y Sellos Electrónicos Cualificados, presta el servicio de validación empleado por la Plataforma de Conservación y almacenamiento a largo plazo.

1.1.5. Sellado Cualificado de Tiempo Electrónico

ANF AC, en su calidad de prestador cualificado de sellos de tiempo electrónico presta el servicio de validación empleado por la plataforma de conservación y almacenamiento a largo plazo.

1.2. Nombre del documento e identificación

Nombre del documento	Servicio cualificado de conservación de firmas y sellos electrónicos cualificados (QEs). Declaración de prácticas del servicio y Política de Conservación		
Versión	1.5.		
OID	1.3.6.1.4.1.18332.61		
Fecha de aprobación	20/02/2025	**Fecha de publicación**	20/02/2025

El identificador de esta política sólo será cambiado si se producen cambios sustanciales que afectan a su aplicabilidad. Esta política es publicada en versión de idioma español e inglés, en caso de discrepancia, prevalece la versión de idioma español.

La entrada en vigor de una nueva versión se produce en el momento de su publicación, la política es publicada en la Web corporativa de ANF AC www.anf.es

1.3. Partes de la PKI

Según lo definido en la DPC de ANF AC.

1.4. Ámbito de aplicación

1.4.1. Usos permitidos

Conservación y almacenamiento de datos, firmas electrónicas avanzadas o cualificadas, y sellos electrónicos avanzados o cualificados, a largo plazo.

1.4.2. Límites de uso

De forma general, según lo establecido en la DPC de ANF AC.

1.4.3. Usos prohibidos

De forma general, según lo establecido en la DPC de ANF AC.

1.5. Datos de contacto del prestador

Según lo definido en la DPC de ANF AC.

1.6. Definiciones y acrónimos

Además de los reseñados en la DPC de ANF AC, a efectos de este servicio se aplican los siguientes términos y abreviaturas,

1.6.1. Definiciones

Autoridad de Sellado de tiempo: ANF AC es el Prestador Cualificado de Sellado de Tiempo de esta política.
Autoridad de Conservación de largo plazo: ANF AC es el Prestador Cualificado que presta este servicio sometido a la presente política.
Autoridad de Validación: Es el Prestador Cualificado que proporciona información sobre el estado del certificado.
Cliente de conservación: aplicación o pieza de software (API) que interactúa con un servicio de preservación a través de un protocolo de comunicaciones.
Conservación a largo plazo: extensión del estado de validez de una firma / sello electrónico durante largos períodos de tiempo y / o extensión de la provisión de pruebas de la existencia de datos durante largos períodos de tiempo, a pesar de la obsolescencia de los componentes criptográficos o de la pérdida de la capacidad de verificar el estado de validez de los certificados de clave pública empleados.
Control dual: procedimiento por el que se requiere la intervención de dos operadores.
Datos: son objetos binarios / octetos reales sobre los que se realiza el proceso de conservación y almacenamiento.
Datos de validación: datos que se utilizan para validar una firma digital.
Dispositivo cualificado de creación de firma electrónica: es un dispositivo que cumple los requisitos enumerados en el anexo II del Reglamento (UE) 910/2014 y que está certificado en tal sentido.
Documento electrónico: es información de cualquier naturaleza en forma electrónica (p.ej. texto de un mensaje, archivo PDF, imágenes, vídeos, etc). En la prestación de este servicio ANF AC garantiza la accesibilidad, confidencialidad, autenticidad, integridad y conservación del documento a largo plazo.
Duración de las evidencias: es el tiempo previsto que el servicio de conservación espera que la evidencia pueda usarse para lograr el objetivo de preservación.

Esquema de preservación: conjunto genérico de procedimientos y reglas pertinentes a un modelo de almacenamiento de preservación y uno o más objetivos de conservación (en el caso de esta política el perfil WST) que describen cómo se crean y validan las evidencias de preservación.

Evidencia de conservación: son los eventos obtenidos que se han generado para lograr la preservación de los datos.

Firma AdES nivel LT: Este formato incluye TimeStamping, toda la información de certificación y de revocación (respuesta OCSP firmada) necesaria para validar la firma a lo largo del tiempo.

Firma AdES nivel LTA: Para preservar la integridad de la firma a largo plazo, se define el formato AdES LTA, que incluye un sello de tiempo sobre la totalidad de la firma. Formatos AdES son aquellos que cumplen la regulación del eIDAS (set de estándares europeos), los más utilizados son: CAdES, PAdES, XAdES.

Firma electrónica avanzada: está vinculada al firmante, permite la identificación del firmante, ha sido creado utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y está vinculado con los datos firmados o sellados de modo tal que cualquier modificación ulterior de los mismos es detectable. La firma electrónica avanzada siempre se genera utilizando un certificado electrónico cualificado vigente y un dispositivo seguro de creación de firma.

Firma electrónica cualificada: es la firma electrónica que cumple los requerimientos establecidos por ley, es decir, ha sido creada empleando un dispositivo cualificado de creación de firmas y un certificado cualificado de firma.

Identificador de objeto de preservación: identificador único de un conjunto de datos enviados a un servicio de preservación.

Interfaz de conservación: componente que implementa el protocolo de preservación en el lado del servicio de conservación.

Largo plazo: período de tiempo durante el cual los cambios tecnológicos pueden ser una preocupación. P.ej. *Los posibles cambios tecnológicos que ocasionan la obsolescencia de la tecnología criptográfica como: cripto-algoritmos, tamaños de clave o funciones hash, etc.*

Metadatos: Son datos encapsulados en otros datos.

Objeto de conservación: objeto de datos mecanografiados que se envía, procesa o recupera de un servicio de conservación.

Perfil / Modelo de conservación: es la forma en la que el prestador del servicio lo implementa, en el caso de esta política el perfil es WST *(conservación y almacenamiento).*

Periodo de retención: el período de tiempo durante el cual las evidencias que se producen de forma asincrónica se pueden recuperar del servicio.

Política de evidencia de conservación y almacenamiento: conjunto de reglas que especifican los requisitos y el proceso interno para generar o cómo validar una evidencia de preservación.

Prueba de existencia: evidencia que prueba que un objeto existió en una fecha / hora específica.

Prueba de integridad: evidencia de que los datos no han sido alterados desde que fueron protegidos.

Re-timbrado / Re-sellado: Aumento de preservación que se realiza sobre una evidencia de conservación a fin de demostrar a largo plazo la existencia de un objeto de conservación determinado, extendiendo así su periodo de validez. P.ej. *Agregar una nueva marca de tiempo que protege los datos de validación adicionales que se pueden utilizar para validar una firma y / o sello de tiempo, y / o el hash de los datos, usando un algoritmo más fuerte.*

Portabilidad: paquete de exportación / importación de la información extraída de un servicio de conservación, incluido el objeto de datos de envío (SubDO), la evidencia de preservación y los metadatos relacionados con la preservación, lo que permite que otro servicio de preservación importe para continuar logrando el objetivo de preservación basado en esta información.

Prestador / Proveedor de servicios de conservación y almacenamiento: En el caso de esta política, ANF AC es el prestador del servicio.

Protocolo de notificación: protocolo utilizado por un servicio de preservación para notificar al cliente de preservación.

Registro de pruebas: Unidad de datos que permite probar la existencia en un momento dado, de un objeto de datos almacenados.

Sello de Tiempo: datos en formato electrónico que vinculan otros datos electrónicos a un momento en particular estableciendo pruebas de que estos datos existían en ese momento.

Servicio de conservación: Servicio capaz de extender el estado de validez de una firma digital durante largos períodos de tiempo y / o de proporcionar pruebas de la existencia de datos durante largos períodos de tiempo.

Servicio de validación: Servicio que valida una firma / sello electrónico, certificados empleados, etc.

Suscriptor / Abonado: es la persona física o jurídica cliente que contrata a ANF AC el servicio de conservación a largo plazo.

1.6.2. Acrónimos

2FA: Doble Factor de Autenticación (multifactor).

AdES: Advanced Electronic Signature.

AGO: Objetivo de aumento.

LT: Long-time. Largo plazo.

LTA: Long-time archive. Archivo a largo plazo.

OCSP: On-line Certificate Status Protocol.

OTP: One-Time-Password.

PC: Políticas de Certificación.

PCSC: Prestador Cualificado de Servicios de Confianza, en el contexto de esta política ANF AC es el PCSC de referencia.

PKI: Infraestructura de clave pública.

POC: Contenedor de objetos de preservación.

PRP: Protocolo de servicio de conservación.

PSP: Proveedor de servicios de conservación.

SCA: Autenticación reforzada de clientes *(Strong Customer Authentication).*

SigS: Servicio de creación de firmas / sellos electrónicos.

SGSI: Sistema de Gestión de la Seguridad de la Información.

SSL: Capa de puertos seguros. Son protocolos criptográficos, que proporcionan comunicaciones seguras por una red y autentican el servidor que presta servicio.

SubDO: Objeto de datos de envío.

TLS: Seguridad de la capa de transporte. Son protocolos criptográficos, que proporcionan comunicaciones seguras por una red y autentican las partes que intervienen en la comunicación.

TSP: Prestador de Servicios de Confianza.

ValS: Servicio de Validación.

WST: Perfil de servicio de conservación con almacenamiento.

2. Repositorios y publicación de la información

2.1. Repositorios

Según lo definido en la DPC de ANF AC.

2.2. Publicación de la información

Según lo definido en la DPC de ANF AC.

2.3. Frecuencia de actualizaciones

Según lo definido en la DPC de ANF AC.

2.4. Controles de acceso a los repositorios

Según lo definido en la DPC de ANF AC.

3. Requisitos operacionales

3.1. Seguridad de los Sistemas de Gestión de la Información (SGSI)

ANF AC, utiliza un Sistema de Gestión de Seguridad de la Información (SGSI) que ha sido certificado en conformidad con la norma ISO/IEC 27001:2013, asegurando así el cumplimiento de los controles de seguridad en la transmisión frente a riesgos de pérdida, robo, daño o cualquier modificación no autorizada.

El SGSI de ANF AC ha sido desarrollado en conformidad con la ISO/IEC 27002 y como se indica en el Anexo A de la ISO/IEC 27001:2013, soporta la firma, el almacenamiento de objetos identifica objetivos y controles adicionales que cumplen específicamente con los riesgos potenciales asociados con la firma y / o el almacenamiento de objetos relevante adicionales que cumplen específicamente con los riesgos potenciales asociados con la firma y / o el almacenamiento de objetos relevantes.

La política de seguridad de la información cumple con las leyes y regulaciones aplicables en especial los controles de riesgos establecidos en la ETSI EN 319 401 y, en particular, el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, habiendo elaborado una Evaluación de Impacto en Protección de Datos (EIPD) con resultado de nivel de riesgo bajo. Además,

- ANF AC cuenta con una Política de Seguridad de la Información OID 1.3.6.1.4.1.18332.101.80.1
- Políticas para la relación con los proveedores de servicios externos que apoyan a ANF AC en la prestación de sus servicios de certificación, habiendo suscrito contrato formal en el que se establecen deberes responsabilidades.
- ANF AC, gestiona:
  - Plan de Gestión de Riesgos, OID 1.3.6.1.4.1.18333.13.2.1;
  - Evaluación de Riesgos, OID 1.3.6.1.4.1.18332.101.80.6.3;
  - Matriz de Riesgos, OID 1.3.6.1.4.1.18333.101.80.6.1;
  - Plan de continuidad y recuperación de desastres, OID 1.3.6.1.4.1.18332.13.1.1;
  - Plan de cese de la actividad, OID 1.3.6.1.4.1.18332.1.9.1.11.
- Se identifican activos, vulnerabilidades, se evalúan riesgos, probabilidad que se produzcan, grado de impacto que pueden ocasionar y salvaguardas aplicadas por la organización.
- Se clasifican las claves privadas de firma como datos sensibles que deben de ser protegidas por medidas especiales.
- Los objetos de datos están clasificados como datos confidenciales del suscriptor / abonado que es responsable de los mismos. Esta información sólo se revela a personas autorizadas por el suscriptor.

ANF AC mantiene criterios en relación a la información disponible para auditorías, y análisis de incidentes que se puedan producir.
Periódicamente, como mínimo una vez al año, se realizan auditorías internas y externas de acuerdo con un Plan de Auditorías de la organización, auditorías contra normas y estándares internacionales en la materia.
Se gestiona control y detección de incidentes en la plataforma de conservación y almacenamiento a largo plazo.

Se aplica lo establecido en la Política para el reporte y tratamiento de incidentes de seguridad OID 1.3.6.1.4.1.18332.101.45.30

Cualquier interesado puede comunicar sus quejas o sugerencias a través de los siguientes medios:

- Por teléfono: 902 902 172 (llamadas desde España) Internacional (+34) 933 935 946
- Por correo electrónico: info@anf.es
- Cumplimentando el formulario electrónico disponible en el sitio web https://www.anf.es
- Mediante personación en una de las oficinas de las Autoridades de Registro Reconocidas.
- Mediante personación en las oficinas de ANF AC.

- ANF AC dispone de un Registro de Incidentes en el que se inscribe toda incidencia que se haya producido con los certificados emitidos, y las evidencias obtenidas. Estos incidentes se registran, analizan y solucionan según los procedimientos del Sistema de Gestión de la seguridad de la Información de ANF AC.
- El Responsable de Seguridad determina la gravedad del incidente y nombra un responsable y, en caso de incidentes de seguridad relevantes, informa a la Junta Rectora de la PKI.
- ANF AC dispone de una Política de Seguridad Física y Ambiental OID 1.3.6.1.4.1.18332.101.45.14 que, entre otras cuestiones, establece requerimientos de acceso físico a las instalaciones de la organización y uso de los activos.
- Los sistemas informáticos de la organización disponen de controles para proteger contra ataques y software malicioso. Se cuenta con procedimiento de control de versionado, control de proyectos y todos los procesos y tecnología están documentados y clasificados.
- Periódicamente se realizan escaneos de puertos y comprobación de las configuraciones de servidores y estudio de los log a fin de detectar acciones sospechosas de intentos de acceso o procesamiento de datos no autorizados.
- Los sistemas son actualizados regularmente a las últimas versiones clasificadas como estables y para explotación.
- Los servidores cuentan con avanzada tecnología de control de accesos indebidos, sistema antivirus, firewall, etc. Se realizan controles periódicos de LOG para detectar intentos de agresión.
- Todo el personal se somete a compromiso de confidencialidad y realiza Formación Continua.
- En teletrabajo se exige conexión SSL e identificación mediante certificado cualificado de firma electrónica.
- ANF AC, el Plan de Contingencias y Recuperación de Desastres, es sometido periódicamente a test.

3.2. Uso de la clave privada

Los suscriptores que disponen de certificado cualificado de firma electrónica, pueden enviar los documentos firmados. En caso contrario, como mínimo el suscriptor deberá emplear una aplicación de ANF AC para la

descarga segura de documentos que en su terminal genera hash del objeto de datos e incluye protocolo de comunicaciones SSL para su envío a la plataforma de conservación.

ANF AC firma los documentos electrónicos con su propia clave en nombre de los suscriptores.

La clave privada de firma se almacena como mínimo en un dispositivo seguro de creación de firma certificado EAL 4+ Common Criteria, aunque por el dispositivo empleado puede estar además certificado en conformidad QSCD conforme al Reglamento eIDAS, en cuyo caso las firmas electrónicas son firmas cualificadas.

Las firmas / sellos electrónicos elaborados en la plataforma de conservación y almacenamiento son firmas de larga vigencia LT / (en conformidad con las normas Baseline).

3.3. Mantenimiento de la firma durante el periodo de almacenamiento

Con el objetivo de asegurar que las firmas/sellos electrónicos se mantengan de manera que se pueda verificar su validez para todo el periodo de almacenamiento. ANF AC ha implantado procedimientos técnicos y medidas organizativas, como mínimo:

a) Medidas técnicas

Todas las firmas incluyen información que permite realizar la validación de la firma *(por ejemplo, la ruta del certificado de un punto de confianza conocido, por ejemplo, CA raíz e información de revocación)* y un indicador de confianza *(por ejemplo, sello de tiempo)* del momento en que esa firma existía y era válido el certificado empleado. La información se almacena al mismo tiempo que el objeto de datos firmado, de tal forma que se garantiza la integridad de este conjunto de información.

Para la transmisión de los datos, la plataforma dispone de los siguientes clientes de conservación:

- Aplicación Web para usuarios personales,
- API para automatización entre sistemas.
-

Ambos sistemas requieren credencial de las partes y se utiliza protocolo de comunicaciones que garantiza la confidencialidad de los datos (SSL).

Todos los objetos de datos recibidos que están firmados, son sometidos a control de validación, solo se aceptan aquellos cuya validación está en conformidad.

Los objetos de datos recibidos y cuya conservación y almacenamiento han sido aceptados, son firmados electrónicamente AdES LT por ANF AC. Se realiza entrega al suscriptor de un acta de aceptación de conservación y almacenamiento OID 1.3.6.1.4.1.18332.62.4

La duración de la evidencia queda determinada por lo establecido en la ETSI TS 119 312. Con el fin de garantizar la preservación de la información autenticada, por un tiempo superior al tiempo de vida de los algoritmos criptográficos y longitudes de clave empleadas, cuando es necesario se aplica proceso

de re-timbrado mediante el empleo de sellos de tiempo de archivo, en conformidad con los estándares ETSI para los formatos de firma AdES, aplicando componentes criptográficos en conformidad con la ETSI TS 119 312

Se gestiona un sistema de LOG que registra todos los eventos de acceso y servicios requeridos y prestados.

b) Medidas organizativas
La plataforma de almacenamiento la mantiene ANF AC, utilizando CPD de multinacionales de reconocido prestigio y garantías. Todos los servidores se encuentran bajo su exclusiva administración y control, instalados en territorio de un país miembro de la Unión.

ANF AC gestiona equipamiento y sistemas que garantizan la capacidad de procesamiento y almacenamiento requerida por sus suscriptores. Se garantiza el servicio con un nivel de SLA superior al 99 %.

3.4. Acceso a la información, publicación y trazabilidad

La información está permanentemente accesible y se han implantado controles de acceso que garantizan que solo personal autorizado puede acceder a ella.

Todas las personas autorizadas para acceder a la información estarán dotadas de credenciales basadas en certificados cualificados de firma electrónica.

El acceso a la información se realiza de forma remota electrónica. La privacidad de las comunicaciones está garantizada mediante el empleo de protocolo de comunicaciones SSL / TLS, en conformidad con la legislación vigente.

Los operadores autorizados, previo al acceso a la información, firman un acta que detalla la solicitud y acciones llevadas a cabo.

Los sistemas disponen de procedimientos para realizar una búsqueda de datos y su publicación.

3.5. Autenticidad e integridad

Con el fin de garantizar la autenticidad del origen y la integridad de un conjunto de objetos de datos, y también con el fin de evitar la pérdida o adición subrepticia, solo es posible el acceso a la información para consulta u obtención de una copia autenticada de la misma.

ANF AC garantiza:

- Previo a la publicación de la información se comprueba validez de la firma que autentica y garantiza su integridad, mediante este procedimiento se detecta cualquier rotura de integridad.

- Toda la información almacenada está autenticada como mínimo con firma electrónica avanzada de larga vigencia en formato AdES LT.
- Se aplican las técnicas necesarias (en caso necesario re-timbrado empleando procedimiento criptográfico fuerte) para garantizar el mantenimiento de la firma durante todo el periodo de almacenamiento.

3.6. Firma

Se aplica lo definido en la Política de Firma de ANF AC OID 1.3.6.1.4.1.18332.27.1.1

3.7. Validación de firma

Se aplica lo definido en la Política de Validación Cualificada de ANF AC OID 1.3.6.1.4.1.18332.56.1.1

Para la validación de las evidencias de preservación se debe de emplear mecanismos de validación cualificada. ANF AC pone a disposición pública mecanismo de validación que permite validar la evidencia electrónica incluyendo:

- Firmas electrónicas.
- Sellos de tiempo electrónico.
- Certificados (cadena de certificación completa)

3.8. Sellado de tiempo electrónico

Se aplica lo definido en la Política de Sello Cualificado de Tiempo Electrónico de ANF AC OID 1.3.6.1.4.1.18332.15.1

3.9. Legibilidad

La plataforma de conservación de largo plazo de ANF AC, solo acepta documentos electrónicos en los formatos PDF, JPG, JPEG, PNG. El servicio no incluye proceso de conversión de objeto analógico a formato digital/electrónico.

Con el fin de garantizar que los objetos de datos sigan siendo legibles por humanos o máquinas durante el período de almacenamiento, se aplican medios técnicos y organizativos:

a) Medidas técnicas

- La plataforma de conservación está configurada para rechazar todos objetos de datos cuyo formato no es aceptado según especificación publicada en la misma plataforma.

- La plataforma de conservación y almacenamiento a largo plazo, incluye sistema de visualización de los documentos y firmas electrónicas.
- Cuando existe el riesgo que un sistema de visualización específico se vuelva obsoleto, todos los datos afectados se copiaron de manera confiable manteniendo su semántica y sin cambios de contenido a un nuevo archivo de datos en formato vigente. Se elaborará una declaración confiable independiente que dé fe de la correspondencia del contenido y la semántica del nuevo objeto de datos con el anterior.

b) Medidas organizativas

ANF AC dispone de un Plan de Calidad que determina procedimiento y operadores que asumen la responsabilidad de verificar la calidad de los documentos electrónicos, previo a su entrega a la plataforma de conservación a largo plazo. Este Plan de Calidad, además de contemplar control de legibilidad incluye control de metadatos que facilitan la búsqueda de los documentos electrónicos.

3.10. Seguridad de la información

Con el objetivo de asegurar que los medios donde se almacenan los objetos de datos puedan soportar el paso del tiempo, como por ejemplo el deterioro del soporte que los almacena o incluso, ataques hacker o corrupción fortuita de la información y, en especial la obsolescencia de los componentes criptográficos empleados para su conservación, se cuenta con:

- sistema de almacenamiento S3, mediante tecnología buckets. Esta tecnología genera automáticamente en línea, copias de soporte del 100 % de los objetos de datos. Estas copias se encuentran en servidores instalados en distinta zona geográfica a los datos en explotación.
- Privacidad. Toda la información almacenada se encuentra protegida criptográficamente para evitar su manipulación. Mediante tecnología SSE-S3, cada objeto se cifra con una clave exclusiva. Como medida de seguridad adicional, cifra la propia clave con una clave maestra que rota periódicamente. El algoritmo criptográfico simétrico empleado es Advanced Encryption Standard de 256 bits (AES-256).
- En el momento de recepción de la información, previa a su aceptación, se procede a comprobar mediante antivirus que el objeto de datos no contiene código malicioso conocido.
- En el momento de recepción de la información, previa a su aceptación, se procede a comprobar si los datos están firmados y, en su caso, se procede a la validación de la firma. En caso de no conformidad se rechaza la conservación.

- En caso de aceptación de conservación, se procede se estampa sello electrónico de larga vigencia de ANF AC, se registra los componentes criptográficos empleados a fin de realizar un control de obsolescencia y, en su caso, re-timbrar aquellos que sean necesarios, y se expide acta de aceptación.
- Cuando se realiza un almacenamiento de objetos de datos cuyo formato puede incluir cambios en la presentación o cualquier modificación no detectable por controles de integridad, la plataforma de conservación notifica al usuario, previo a su publicación, que los objetos de datos que están en un formato poco fiable.

3.11. Requisitos de separación y confidencialidad

Con el objetivo de garantizar la confidencialidad de la información, los objetos de datos electrónicos relacionados con diferentes organizaciones de propietarios se almacenan y archivan de forma que resulte imposible su acceso a terceros no autorizados. Cada objeto de datos cuenta con un identificador exclusivo de su propietario (código de suscriptor) y se restringe el acceso a los datos en función de su propietario.

3.12. Protocolo de conservación

El servicio ha sido desarrollado por el departamento de I+D de ANF AC y dispone de su propio protocolo de conservación. Funciona con XML. Está protegido contra el uso no autorizado.

En concreto las operaciones indicadas por la ETSI TS 119 512:

- RetrieveInfo
- PreservePO
- RetrievePO
- DeletePO
- UpdatePOC
- RetrieveTrace
- ValidateEvidence
- Search

Se puede obtener los rastros de todas las operaciones relacionadas con un identificador de objeto de preservación específico, tal y como se define en la operación *RetrieveTrace* según ETSI TS 119 512

Es posible buscar objetos de preservación incluyendo filtros y recuperarlos tal y como se define en la operación *Search* según ETSI TS 119 512

En el caso de que el suscriptor solicite la eliminación de una orden de conservación antes de finalizar el periodo de conservación, se requerirá que la solicitud sea formulada por una persona autorizada por el suscriptor y que facilite el correspondiente justificante.

La eliminación tiene un alcance a los objetos de datos y las pruebas de conservación de la SubDO.

La eliminación no conlleva necesariamente la destrucción de la información, el contrato de suscripción del servicio establecerá si el alcance de una eliminación es destrucción o el bloqueo de los datos.

En caso de bloqueo de datos, se eliminará la información del repositorio del servicio de conservación y se almacenará una copia en un repositorio de seguridad, aplicando una limitación de uso con el fin de hacerla inaccesible. La información con limitación de uso, tiene como único objetivo acreditar la correcta prestación del servicio por parte de ANF AC, o atender una orden de un Tribunal de Justicia.

3.13. Protocolo de notificación

De cada entrega de objeto de datos realizada por el suscriptor, el servicio de Conservación genera un acta en la que se especifica si el servicio ha sido aceptado o rechazado y, en su caso, validación de firma/sello o generación de sello electrónico de ANF AC. En caso de rechazo se especifica la causa.

El suscriptor bajo demanda puede descargar objeto de datos, evidencia de preservación o actas anteriormente indicadas mediante la consola del servicio. Solo accesible a personas autorizadas por el suscriptor.

No está previsto realizar notificación.

3.14. Informes e intercambios con las autoridades

El propietario es el suscriptor del servicio de los documentos electrónicos almacenados, por ello, salvo en caso de mandato judicial, el acceso y publicación de los datos a las autoridades deberá ser autorizado por el propietario de los datos.

Con el fin de asegurar que los objetos de datos se informan e intercambian con las autoridades autorizadas por el propietario, de tal manera que se garantiza la integridad y seguridad de la fuente de datos, ANF AC garantiza:

- El representante de la autoridad debe de identificarse de acuerdo con lo establecido en esta política de certificación y se le dotará de credenciales de acceso, cuyo uso deberá adecuarse a esta política, a la DPC de ANF AC.
- Se utiliza canal seguro para el envío de objetos de datos a las Autoridades, de modo que el usuario remoto y el servidor está autenticado, la integridad y la confidencialidad de las comunicaciones están protegidas sobre vulnerabilidades de las redes. (por ejemplo, credenciales de usuario y protocolo de comunicaciones SSL).
- El acceso a la información es remoto, disponible 24x7x365.
- La plataforma de publicación ofrece la posibilidad de lectura y obtención de copias auténticas de los documentos electrónicos de interés.
- Previa a la publicación se realiza validación de las evidencias de conservación.

4. Roles de confianza

Todo el personal que participa en la gestión y administración de la plataforma de conservación, ha sido claramente informado por escrito de sus deberes y responsabilidades, este personal ha aceptado por escrito las responsabilidades y obligaciones.

Además, el personal de ANF AC ha suscrito el correspondiente compromiso de confidencialidad, compromiso que perdura incluso después de su salida de la organización.

Periódicamente ANF AC realiza auditoría interna de procesos y de la actividad desarrollada por su personal a fin de reducir el riesgo de robo, fraude o mal uso de los activos de la organización.

Todo el personal de ANF AC ha recibido credenciales basadas en certificado cualificado de firma electrónica, y formación específica en el campus de ANF AC para el adecuado desempeño de sus funciones.

ANF AC dispone y aplica políticas de RRHH:

- Política de Roles y responsabilidades OID 1.3.6.1.4.1.18332.38.1,
- Normativa Interna OID 1.3.6.1.4.1.18332.101.80.5
- Plan de formación OID 1.3.6.1.4.1.18332.100.20.1.2

4.1. Controles de personal

Según lo definido en la DPC de ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1, Políticas de RRHH y específicamente:

Las personas que participan en los servicios prestados por ANF AC, son personal que se encuentra bajo la dirección de la organización, y son seleccionados conforme a criterios objetivos de capacitación y disponibilidad.

Se han establecido funciones exclusivas de personal de alta confianza de la alta dirección de ANF AC:

Responsable de verificación de identidad

Es personal adscrito al área RDE de ANF AC. Asume la responsabilidad de asegurar el cumplimiento de los procesos establecidos para la verificación de la identidad inicial del suscriptor y operadores autorizados a acceder en su nombre.

Administrador de sistemas
Es personal adscrito al área técnica de ANF AC. Asume la responsabilidad de asegurar la plena operatividad de los sistemas, realizar labores de instalación, configuración, mantenimiento para la gestión de los servicios. Requerimientos específicos:

- No tienen acceso a las claves de la CA.
- No tienen acceso a los LOGs de la CA. Se evitará mediante propiedades del usuario del software de CA.

- Se autentifican vía SmartCard o token USB con el software de CA y no admitirá este software otro método alternativo de autenticación.

Responsables de claves de acceso al QSCD

Son los encargados de la activación de las claves de firma del ERDS, cada responsable dispone de una SmartCard o un Token USB que permiten gestionar las claves de firma conservadas en un dispositivo QSCD en servidor de firma a distancia. El número de responsables de claves de accesos de tres personas, y el sistema requiere intervención dual.

Este personal de confianza es el único autorizado y habilitado para realizar sobre la clave de firma operaciones de copia de respaldo, conservación y recuperación. Siempre bajo control dual y en un ambiente físicamente seguro.

Operador de sistemas

Personal autorizado a utilizar los terminales con acceso a los sistemas de entrega certificada y que realizan labores generales de gestión y atención diaria del servicio. Este rol no es incompatible con el de administrador de sistemas.

Auditor del sistema

Autorizado a ver archivos y auditar los LOGs de los sistemas de ANF AC.

Los logs los verá a través de la interfaz web que ofrece la CA. Autenticación a través de SmartCard o token.

Sólo tendrá acceso a los logs este Rol.

El auditor debe encargarse de:

- Comprobar el seguimiento de incidencias y eventos
- Comprobar la protección de los sistemas (explotación de vulnerabilidades, LOGs de acceso, usuarios, etc.).
- Comprobar alarmas y elementos de seguridad física

Responsable de Seguridad

De acuerdo con lo definido en la Política de Seguridad de ANF AC. Además, se encargará:

- Constatar la existencia de toda la documentación requerida y numerada
- Comprobar la coherencia de la documentación con los procedimientos, activos inventariados, etc.

4.2. Proveedores y colaboradores externos

ANF AC ha elaborado una Política de relación con los proveedores y colaboradores externos que requiere un análisis de evaluación que determine su adecuación para el rol que precisa la organización.

Código de conducta de miembros y proveedores OID 1.3.6.1.4.1.18332.101.45.1

La relación con estas entidades siempre se formaliza contractualmente. Los contratos entre otras cláusulas incluyen compromiso de confidencialidad y, una vez finalizada la relación, exigencia de devolución de los activos de la organización y retirada de las credenciales de acceso que se les pudiera haber otorgado.

Suscriptores /Abonados

Personas físicas o jurídicas que contratan este servicio de conservación y almacenamiento a largo plazo.

Terceros que confían

Todas aquellas personas que, de forma voluntaria, confían en los servicios prestados por ANF AC aceptando los términos y condiciones del servicio, así como las limitaciones de uso, Políticas y Prácticas de ANF AC.

5. Identificación y autenticación

5.1. Identificación inicial

La identidad del suscriptor/abonado y sus operadores autorizados, así como la de los operadores de ANF AC encargados de la administración de la plataforma, se verificará por uno de los medios de identificación de nivel de seguridad sustancial o nivel de seguridad alto (1) siguientes:

- Presencia física en una de las Oficinas de Verificación Presencial o AR de ANF AC, o bien por medio de un tercero de conformidad con el Derecho nacional.
- Mediante un certificado de una firma electrónica cualificada o de un sello electrónico cualificado vigente.
- Utilizando alguno de los procedimientos establecidos en el art. 24 del Reglamento eIDAS.
- Mediante un medio de 2FA en el que uno de los factores se base en un procedimiento calificado por Tribunal de Justicia o legalmente reconocido a escala nacional como medio que permite la identificación de una persona física.

La identidad de los terceros que confían (auditores, inspectores de AEAT, y operadores autorizados expresamente por el suscriptor) se podrá realizar mediante uno de los medios de identificación de nivel de seguridad bajo (2).

(1) *Art. 8.2. del Reglamento eIDAS*

5.2. Autenticación

El proceso de autenticación se realizará mediante Certificado Cualificado de Firma Electrónica.

6. Procedimiento funcional

El servicio aplica los métodos de identificación, firma o sello electrónico, verificación OCSP y sello cualificado de tiempo electrónico previstos en el Reglamento eIDAS, sometiendo los documentos electrónicos a permanentes auditorías a fin de garantizar la integridad, autenticidad y legibilidad de los archivos custodiados a lo largo del tiempo.

Este servicio es prestado durante el periodo de tiempo contratado por el suscriptor cliente, finalizada la contratación la información es bloqueada o destruida de forma definitiva (ver sección 3.12).

El servicio de conservación garantiza un acceso permanente, la plena recuperación de los documentos, y la gestión de las evidencias que permiten demostrar la integridad de los documentos custodiados.

6.1. Descarga de objeto de datos

La plataforma de conservación dispone de dos procedimientos para que los suscriptores puedan transmitir los objetos de los datos. Los clientes de conservación disponibles son:

a) Consola de usuario final en servidor Web.
b) API para establecer comunicación entre el sistema automatizado del suscriptor y la plataforma de conservación de ANF AC.

En cualquiera de los supuestos se utiliza protocolo de comunicaciones SSL/TLS para garantizar la privacidad de los datos y el suscriptor utiliza credenciales para autenticarse ante la plataforma de conservación.

Se permite que uno o más objetos de datos de envío (SubDO) se conserven bajo un perfil de preservación específico.

6.2. Protección inicial

Con el fin de garantizar integridad y un control adecuado del proceso de auditoría, la plataforma en el momento de recepción del documento electrónico, realiza:

- Comprobación de identidad del suscriptor. Solo suscriptores del servicio pueden enviar datos.
- Comprobación de validez del formato del objeto de datos. Solo formatos aceptados por la plataforma pueden ser aceptados.
- En caso de que el documento electrónico esté firmado, se procederá a realizar validación de la firma o sello electrónico que lo autentican. En este proceso se utiliza un sistema cualificado de validación de firmas y sellos electrónicos.
- En caso de que el documento electrónico se transmita asociado a un hash, se comprobará la correspondencia del hash con el objeto de datos.
- Se obtiene evidencia de la conformidad o fallo del proceso de validación de firma o hash realizado en los anteriores pasos. En caso de no conformidad se realiza una denegación de servicio.

- Se registran metadatos del documento.
- La plataforma aplica una firma/sello LTA al documento electrónico a fin de asegurar integridad, vigencia a largo plazo, y unificar proceso de auditoría permanente.
- La firma aplicada como mínimo es una firma electrónica avanzada elaborada con un certificado cualificado, y conforme con los estándares ETSI AdES.
- Se incluye sello cualificado de tiempo electrónico en conformidad eIDAS, y verificación de estado en origen por consulta OCSP, ambos emitidos por ANF AC en calidad de PCSC.
- El documento y evidencias obtenidas de los anteriores procesos es almacenado en carpeta específica individualizada para ese suscriptor.
- La información es almacenada en zona de explotación y replicada en zona de recuperación, servidor backup situado en diferente ubicación geográfica

6.3. Acceso a la información, trazabilidad.

La plataforma de conservación y almacenamiento a largo plazo, gestiona un servicio de metadatos que facilita su búsqueda y localización. Los metadatos incluyen información relativa del sistema que genera la evidencia. Además, se gestiona un procedimiento que gestiona la trazabilidad de los datos: operadores que han accedido, acciones llevadas a cabo y el momento en que se produjo cada evento.

Cada operador debe de firmar un acta de acceso, asumiendo de esta forma su responsabilidad en la transacción realizada. La plataforma dispone de sistema de búsqueda y publicación, desde un entorno web privado y disponible 24x7x365.

6.4. Expediente

La plataforma permite asociar documentos mediante un identificador exclusivo, de esta forma puede acceder a todos los documentos correspondientes a un mismo expediente de forma sencilla y eficaz.

6.5. Augmentación

Auditoría en línea: previa a la publicación de un documento, se realiza una validación de firma, en caso de conformidad se da acceso al suscriptor. En caso de fallo se procede a restaurar una copia del backup una vez verificada integridad.

Periódicamente se realiza una auditoría de integridad de todos los documentos almacenados.

Re-timbrado: se realiza un seguimiento de la evolución del estado de la técnica y de la seguridad de los algoritmos y procedimientos criptográficos empleados en su autenticación, en caso de entrada en riesgo, se procede a re-sellar las evidencias aplicando un sello cualificado de tiempo electrónico que utilice componentes criptográficos calificados como seguros en conformidad con la ETSI TS 119 312.

6.6. Protección

Las claves de firma se encuentran físicamente aisladas de las operaciones normales, de tal manera que solo el personal de confianza designado tenga acceso a las claves para su uso en la firma del contenido y / o evidencia del usuario.

Las claves de firma se conservan y utilizan como mínimo, en un dispositivo seguro de creación de firma, o un dispositivo cualificado de creación de firma (QSCD). Las copias de seguridad de las claves de firmas se almacenan en bunker bancario.

Se aplican medidas de seguridad durante el transporte y almacenamiento de los dispositivos criptográficos empleados por el servicio ERDS, realizando los test necesarios que garantizan su correcto funcionamiento previo a su puesta en explotación.

Los ficheros de registro, se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico. Las evidencias almacenadas en sistemas de almacenamiento S3, mediante la tecnología buckets.

Se generan copias de soporte completas de registro de auditoría, protegidas criptográficamente para evitar su manipulación. Mediante tecnología SSE-S3, cada objeto se cifra con una clave exclusiva. Como medida de seguridad adicional, cifra la propia clave con una clave maestra que rota periódicamente, el algoritmo criptográfico simétrico empleado es Advanced Encryption Standard de 256 bits (AES-256).

Se generan registros de eventos (LOGs) que permiten establecer la información necesaria para pruebas de auditoría.

Las comunicaciones con los sistemas siempre se realizan utilizando protocolo de comunicaciones cifradas SSL entre los usuarios y los sistemas de ANF AC, y TLS entre sistemas informáticos.

6.7. Portabilidad - Importación

El suscriptor puede solicitar la portabilidad de los datos almacenados en la plataforma de conservación, o la importación de datos. La información será entregada o recibida en un formato estandarizado *(siempre basado en un formato abierto*), o en alguno de los formatos definidos en Anexo TR-ESOR-F de BSI de la Guía técnica BSI 03125 para la preservación de evidencias criptográficas, publicado en,

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03125/PrevVersion-1_2/BSI_TR_03125_TR-ESOR-F_V1_2_EN.html

La portabilidad o importación de datos no es automatizada. Se realizará presupuesto previo cuyo costo dependerá del volumen y complejidad de la información, la prestación de servicio requerirá su aceptación por parte del suscriptor.

Trámite de solicitud:

- Debe ser solicitada por el representante legal del suscriptor:
  - La solicitud deberá ser remitida por correo electrónico a soporte@anf.es y estará firmada electrónicamente.
  - Indicará el tipo de formato en el que desea recibir o enviar los datos.
  - Indicará la persona o personas autorizadas para descargar o enviar la información.
  - Abonará las tasas que previamente haya aceptado por presupuesto emitido por ANF AC.

El paquete de datos importados o portados será transmitido cifrado a través del servicios Security Transfer de ANF AC.

Los paquetes de datos exportados sólo serán entregados a la persona autorizada por el suscriptor del servicio.

Se gestionará un registro de todos los paquetes de datos portados, ya sea exportados o importados especificando:

1) La fecha del evento.
2) Los criterios que se han utilizado para seleccionar el conjunto de objetos de preservación que se incluirán en la exportación-importación.

6.8. Fin del periodo de conservación

La prestación del servicio establece un perfil WST *[conservación y almacenamiento].* El plazo de duración se corresponde al periodo contratado por el suscriptor.

Finalizado el plazo y concluida la relación contractual con el suscriptor en caso de no renovación del servicio, se comunica al suscriptor que los datos serán destruidos y se pone a su disposición, durante un periodo de 60 días la portabilidad (exportación de los datos).

7. Perfil de conservación

Este perfil de conservación está identificado unívocamente con el OID 1.3.6.1.4.1.18332.61.10.

La Política de Conservación que se aplica en este Perfil de Conservación en el momento de su publicación es, OID 1.3.6.1.4.1.18332.61.

La Política de Validación que se aplica en este Perfil de Conservación en el momento de su publicación es, OID 1.3.6.1.4.1.18332.56.1.1.

La versión de las citadas políticas puede cambiar con el tiempo y son públicamente accesibles en http://www.anf.es (última versión e histórico). Se aplicará la versión que corresponda al momento de generar la evidencia de conservación.

7.1. Metas de la conservación

La plataforma de conservación de ANF AC está diseñada y desarrollada para obtener los siguientes objetivos:

- **Preservación de datos generales (PGD):** proporciona una prueba de existencia durante largos períodos de tiempo del objeto de datos de envío (SubDO) enviado al servicio de conservación. Alcanza tanto a datos firmados como no firmados.
    - *http://uri.etsi.org/19512/goal/pgd*
- **Preservación de firmas digitales (PDS):** extiende durante largos períodos de tiempo la capacidad de validar una firma / sello electrónico, mantener su estado de validez y obtener una prueba de la existencia del asociado datos firmados.
    - *http://uri.etsi.org/19512/goal/pds*
- **Preservación Aumentada (AUG):** indica que el servicio de preservación admite el aumento de las evidencias de conservación enviadas (re-timbrado).
    - *http://uri.etsi.org/19512/goal/aug*

7.2. Modelo de almacenamiento

La plataforma de conservación de ANF AC almacena los objetos de datos que le son enviados por los suscriptores (SubDO), así como las evidencias de preservación que son producidas por el servicio de conservación. En este modelo, el servicio de conservación apoya la portabilidad e importación de objetos de preservación y evidencias producidas por la propia plataforma o de terceros proveedores según el caso.

El servicio de conservación de ANF AC contempla un único modelo de almacenamiento, WST.

El modelo de almacenamiento de ANF AC es almacenamiento WST, en conformidad con la cláusula 4.3 ETSI TS 119 512. Los datos a conservar son almacenados y se entregan a petición del cliente, junto con las evidencias.

El cliente envía el objeto de datos completo al servicio de conservación.

Este modelo de almacenamiento se aborda mediante el valor WithStorage (WST) dentro de PreservationStorageModelType.

```
<simpleType name = " PreservationStorageModelType " >
        < base de restricción = " cadena " >
                <enumeration value = " WithStorage " />
        </restriction>
</simpleType>
```

Se aplicará el mismo perfil de conservación durante todo el período de conservación al objeto de datos y a la evidencia de conservación.

7.3. Identificador

El modelo de almacenamiento de ANF AC se aborda mediante el valor WithStorage (WST) dentro del PreservationStorageModelType. En conformidad con

- http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers

7.4. Operaciones compatibles

La plataforma de ANF AC soporta:

- Conservación,
- Recuperación,
- Borrado,
- Validación,
- Búsqueda.

7.5. Generación y validación de evidencias de conservación

La plataforma de ANF AC soporta dos tipos de SubDO:

- SubDO con una o más firmas digitales (SubDOwithDS)

  - SubDOwithDS, el servicio de conservación realizará una validación de firma de acuerdo con la política de validación de ANF AC, y recopile y almacene los informes de validación en repositorio al efecto.
- SubDO sin firmas digitales (SubDOwoDS)
  - Se procede a la obtención de una evidencia de conservación elaborada mediante sello electrónico AdES LT de ANF AC.

En cualquier caso, la evidencia de conservación producida será un formato de archivo de una firma AdES.

7.6. Aumento de evidencias de conservación

Se sigue lo establecido en la ETSI TS 119 312 a efectos de seguridad criptográfica.

El servicio de re-timbrado de ANF AC realiza sellos cualificados de tiempo electrónico para incrementar la seguridad criptográfica en caso de necesidad.

7.7. Esquema del perfil

El servicio de ANF AC se ha diseñado y desarrollado de acuerdo con el siguiente esquema de perfil WST "Conservación y almacenamiento".

- *ProfileIdentifier*: Se identifica de forma única el perfil del servicio, es WST.
- *Operation*: Se informa de las operaciones compatibles (3.2), el sistema contempla los elementos:
  - *Input / Format / FormatID* correspondiente a la operación PreservePO contiene el URI http://uri.etsi.org/19512/format/DigestList, y
  - los elementos Input / Format / Parameter / Format / FormatID especifican el conjunto de resúmenes admitidos algoritmos.
- *Policy*: La política de conservación de evidencias se encuentra en el documento OID 1.3.6.1.4.1.18332.61.11. La política de validación de firma se encuentra en el documento OID 1.3.6.1.4.1.18332.56.1.1.
- *ProfileValidityPeriod*: el punto en el tiempo a partir del cual el perfil de conservación se ha activado es el momento en que se acepta el objeto de datos y se aplica sello electrónico de ANF AC. El periodo de conservación finaliza y se desactiva en el momento de concluir la obligación contractual con el cliente.
- *PreservationStorageModel*: es igual a WithStorage.
- *PreservationGoal* – De acuerdo con lo especificado en el apartado 7.1 de este documento.
- *EvidenceFormat*: Firma AdES LT.
- *Specification*: No se requiere.
- *Description*: No se requiere.
- *SchemeIdentifier*: No se requiere.
- *PreservationEvidenceRetentionPeriod*: Duración del contrato suscrito con el suscriptor, más 60 días para realizar portabilidad en caso de ser requerida por el suscriptor.
- *Extension*: No se requiere.

8. Obligaciones y responsabilidades

8.1. Obligaciones del prestador del servicio

ANF AC, en su calidad de Prestador Cualificado de Servicios de Confianza, asume íntegramente la provisión de todos los servicios QTSP necesarios para la prestación del servicio de conservación a largo plazo. Se obliga a:

- Respetar lo dispuesto en esta Política.
- Implementa controles de seguimiento ETSI TS 119312
- Se realiza un control del estado de la técnica criptográfica y sus avances.
- Proteger sus claves privadas de forma segura.
- Emitir sellos cualificados de tiempo electrónico cuyo contenido mínimo sea el definido por la normativa vigente.
- Tramitar y emitir certificados cualificados de firma electrónica.
- Tramitar y emitir certificados cualificados de sello electrónico.
- Tramitar y emitir certificados de sello de tiempo electrónico.
- Tramitar y emitir certificados de OCSP.
- Servicio a distancia de firma electrónica cualificada.
- Obtener respuestas OCSP firmadas por el PCSC emisor cuyo contenido mínimo sea el definido por la normativa vigente.
- Proceder a la validación de las firmas y sellos electrónicos mediante un servicio cualificado de validación en conformidad con la normativa vigente.
- Publicar esta Política en web corporativa.
- Informar sobre las modificaciones de la Política a suscriptores clientes.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.
- Responder por el incumplimiento de lo establecido en esta política y, allí donde sea aplicable.
- Todas las personas que intervienen en la gestión y administración del servicio, están obligadas a guardar secreto de toda la información gestionada por ANF AC, habiendo suscrito el correspondiente compromiso de confidencialidad.
- Garantizar la confidencialidad de las comunicaciones y de los documentos electrónicos custodiados, utilizando para ello técnicas de cifrado fuerte cuando sea de aplicación.
- No se facilitará información relativa a los servicios prestados a terceros, salvo cumplimiento de mandato judicial.

8.1.1. Responsabilidad financiera

Se aplica dentro de los límites establecidos en la vigente Ley de Firma electrónica.

8.1.2. Exoneración de responsabilidad

ANF AC, no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

- Daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en la presente política y en la legislación vigente, donde sea aplicable.
- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el suscriptor cliente o por los Terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento del servicio.
- Por el uso indebido de la información contenida en el Certificado o en la CRL.
- Por el contenido de los mensajes o documentos utilizados.
- En relación a acciones u omisiones del Cliente.
- Falta de veracidad de la información suministrada para la prestación del servicio.
- Negligencia en la conservación de sus datos de acceso al servicio, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- Extralimitación en el uso del servicio, según lo dispuesto en la normativa vigente y en la presente política.

ANF AC, no revisa los contenidos de los documentos electrónicos recibidos para su conservación, interviene como mero proveedor del servicio, por tanto, la intervención de ANF AC no puede presuponer adhesión ni responsabilidad sobre su contenido.

8.2. Obligaciones del suscriptor

- Respetar lo dispuesto en esta Política, Términos y Condiciones, y compromisos asumidos en el Contrato de Prestación de Servicios.
- Proteger las credenciales que le permiten el acceso a la plataforma de conservación de ANF AC.
- Respetar lo dispuesto en los documentos contractuales firmados con ANF AC.
- Reportar cualquier incidente de seguridad tan pronto como este sea identificado.
- Transferir documentos electrónicos que cumplen con los requerimientos técnicos y organizativos establecidos por ANF AC. En especial, cuando transfiere datos autenticados mediante firma electrónica, aplicando firmas electrónicas válidas.
- Está prohibido la aplicación de ingeniería inversa y la búsqueda de fallos en la lógica del sistema.
- Los objetos deben cumplir los requisitos de formato establecidos en el control SS.3.5 del anexo A de la ETSI TS 102 573
- Enviar los objetos de forma precisa y completa, de conformidad con los requisitos establecidos en la Política de Seguridad de la Información de ANF AC.

8.3. Obligaciones de terceras partes que confían

Es obligación de las terceras partes que confían cumplir con lo dispuesto por la normativa vigente y, además:

- Previo a depositar su confianza, proceder a la validación cualificada de las firmas y sellos que autentican las evidencias y documentos probatorios, utilizando un servicio cualificado de firmas y sellos electrónicos.
- Tener en cuenta las limitaciones en el uso del servicio, según lo indicado esta Política de Certificación.
- Reportar cualquier incidente de seguridad tan pronto como este sea identificado.
- Tener en consideración otras precauciones descritas en acuerdos u otros sitios.

9. Cese del servicio

ANF AC cuenta con un Plan de Cese OID 1.3.6.1.4.1.18332.1.9.1.11

9.1. Acciones previas al cese de la actividad

En caso de cese de su actividad como Prestador de Servicios de Confianza, ANF AC realizará las siguientes acciones con una antelación mínima de dos meses, o en un periodo de tiempo lo más corto posible en caso de compromiso, pérdida o sospecha de compromiso de clave privada empleada para autenticar las evidencias y documentos probatorios, así como estampación de sellos cualificados de tiempo electrónico y respuestas de validación OCSP.

9.1.1. Comunicación a interesados

Informar del cese a todos los clientes y otras entidades con las que existan acuerdos u otras formas de relaciones establecidas, entre las que se incluyen proveedores de servicios de confianza y autoridades relevantes como los organismos de supervisión. Además, esta información se pondrá a disposición de otras partes de confianza.

9.1.2. Notificaciones al Organismo de Supervisión

Comunicar al Organismo de Supervisión competente en materia de servicios cualificados eIDAS, el cese de su actividad, así como cualquier otra circunstancia relevante relacionada con el cese de actividad.

Poner a disposición del Organismo de Supervisión competente, información de eventos y logs para que éste se haga cargo de su custodia durante el resto del periodo comprometido.

En virtud del acuerdo establecido con la Asociación de Prestadores Cualificados de Servicios de Confianza de España, depositar información de eventos y logs para que éste se haga cargo de su custodia durante el resto del periodo comprometido y/o legalmente establecido.

9.1.3. Transferencia de obligaciones

Transferir las obligaciones a una parte de confianza para mantener toda la información necesaria para proporcionar evidencia de operación durante un periodo razonable, a menos que se pueda demostrar que ANF AC no dispone de esta información.

ANF AC recopilará toda la información referida, y la transferirá a una parte de confianza con la que se dispone de un acuerdo de ejecución del Plan de Cese en caso de quiebra.

Cuando se produzca un cese de la actividad sin que implique una situación de quiebra, se almacenará toda la información registrada sin necesidad de transferirla a una parte de confianza.

9.1.4. Gestión de las claves de firma del servicio

Destruir tanto las claves privadas como las copias de seguridad de los certificados de firma y sellos electrónicos empleados por ANF AC para la prestación del servicio, de modo que estas no puedan ser recuperadas. Esta operación se ejecutará siguiendo el procedimiento establecido en la política correspondiente.

Las claves de firma siempre se destruirán al retirar el dispositivo criptográfico que las contiene. Esta destrucción no afecta necesariamente a todas las copias físicas de la clave privada. Solo se destruirá la copia física de la clave almacenada en el dispositivo criptográfico en cuestión.

9.1.5. Transferencia de la gestión del servicio

No se contempla la transferencia de la gestión del servicio.

9.2. Obligaciones tras el cese de la actividad

Se realizará:

- notificación a entidades afectadas; y
- transferencia de las obligaciones a otras partes

ANF AC mantendrá disponible su clave pública a las partes de confianza durante un periodo no inferior a quince años.

Estas obligaciones se llevarán a cabo mediante la publicación en la página web https://www.anf.es

si se produce un cese de la actividad sin que implique una situación de quiebra. En caso de que se produzca una quiebra, estas obligaciones serán asumidas por una parte de confianza en virtud del acuerdo establecido con la Asociación de Prestadores Cualificados de Servicios de Confianza de España.

10. Limitaciones de responsabilidad

10.1. Garantías y limitaciones de garantías

ANF AC puede limitar su responsabilidad mediante la inclusión de límites de uso del servicio, y límites de valor de las transacciones para las que puede utilizarse el servicio.

10.2. Deslinde de responsabilidades

ANF AC no asume ninguna responsabilidad en caso de pérdida o perjuicio:

- Daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en la presente política y en la legislación vigente, donde sea aplicable.
- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el suscriptor cliente o por los Terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento del servicio.
- Por el uso indebido de la información contenida en el Certificado o en la CRL.
- Por el contenido de los mensajes o documentos utilizados.
- En relación a acciones u omisiones del suscriptor.
- Falta de veracidad de la información suministrada para la prestación del servicio.
- Negligencia en la conservación de sus datos de acceso al servicio, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- Ocasionados al receptor o terceros de buena fe si el destinatario de los documentos entregados electrónicamente no comprueba ni tiene en cuenta las restricciones que figuran en el servicio en cuanto a sus posibles usos.
- Ocasionados por el uso del servicio que exceda los límites establecidos en el certificado empleado por ANF AC para la prestación del servicio o por la presente política.
- Ocasionados por depositar la confianza sin realizar las validaciones cualificadas requeridas, empleando para ello un servicio cualificado de validación de firmas y sellos electrónicos.

11. Términos y condiciones

ANF AC, pone a disposición de los suscriptores del servicio y de todas las partes que confían, está política que incluye los términos y condiciones en que se presta el servicio de conservación. Este documento está permanentemente publicado en formato PDF y puede ser descargado en,
https://www.anf.es/repositorio-legal/

11.1. Contratación del servicio

El servicio solo es prestado a suscriptores que formalmente han suscrito el correspondiente contrato aceptando estos términos y condiciones, y está política de certificación en su integridad.

La modalidad de servicio prestada corresponde al perfil WST definido en la ETSI TS 119 511 de conservación y almacenamiento de larga vigencia. La duración de la conservación y almacenamiento es por el tiempo de duración del contrato suscrito entre ANF AC y el suscriptor del servicio.

11.2. Constitución del depósito de conservación

Este servicio ofrece una plataforma de conservación y almacenamiento seguro de datos y evidencias a largo plazo. La solución garantiza un acceso permanente y la recuperación integra de los documentos almacenados, gestiona las evidencias que permiten demostrar la integridad de los documentos almacenados.

En el caso de que el suscriptor asuma el compromiso de participar en el proceso de preservación, deberá aportar una forma AdES LTV (validación a largo plazo).

En el caso de que el suscriptor realice entrega de datos que han sido autenticados previamente mediante firma o sello electrónico, ya sea un nivel básico BES, o LT, o LTV, previo a su aceptación el servicio de conservación procederá a su validación. Si el resultado de la validación es INDETERMINADO o TOTAL FALLO, no se aceptará el depósito y se procederá a la destrucción del objeto de datos recibido.

En el supuesto de que no sea posible recopilar y verificar todos los datos de validación, se cancelará la solicitud de conservación y se procederá a la destrucción del objeto de datos recibido.

El servicio de conservación no analiza el contenido de los objetos de datos enviados por el suscriptor para su conservación. En el caso que el objeto de datos sea únicamente un hash, no es posible comprobar la correspondencia de ese hash, ni tan siquiera si corresponde a un hash, ni si el cálculo realizado para su obtención ha sido correcto. ANF AC no es responsable de garantizar la asociación de un hash con documento alguno.

ANF AC apercibe a sus suscriptores que un hash permite probar la existencia de un objeto de datos, pero tan solo mientras que el algoritmo empleado para su obtención es seguro.

11.3. Disponibilidad de los documentos electrónicos

Una vez constituida la entrega, la plataforma de conservación WST mantiene la custodia del documento y asume el control de acceso al mismo y la larga vigencia de preservación, la disponibilidad es permanente vía electrónica.

11.4. Portabilidad - Importación

Según se especifica en la sección 6.7 “Portabilidad – Importación” de este documento.

11.5. Disponibilidad del servicio

La plataforma estará disponible durante las 24 horas del día, los 7 días de la semana, entendiendo por disponibilidad, la capacidad de acceder al servicio por parte del usuario autorizado que lo demanda, con independencia de la rapidez o ritmo al que posteriormente éste sea prestado, y siempre previa identificación con conformidad.

Esta disponibilidad, medida en el periodo de un mes, en ningún caso podrá ser inferior a un 99,9%.

Los Términos y Condiciones del acuerdo de nivel de servicio, se encuentran detallados en el documento SLA *(Service Level Agreement)*.

11.6. Seguridad del Sistema de Gestión de la Información

ANF AC garantiza autenticidad, integridad de la información, control de acceso exclusivo a personas debidamente autorizadas, y su confidencialidad.

11.7. Términos legales

La relación entre ANF AC y el suscriptor del servicio se rige exclusivamente por la legislación española.

Explícitamente se asumen como de aplicación las siguientes normas:

- Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre

circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.
- Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza.

11.8. Resolución de conflictos

Toda controversia derivada de este contrato o acto jurídico, así como los que del mismo deriven o guarden relación con él -incluida cualquier cuestión relativa a su existencia, validez, terminación, interpretación o ejecución- será resuelta definitivamente mediante arbitraje de Derecho, administrado por el Tribunal de Arbitraje del Consejo Empresarial de la Distribución (TACED), de conformidad con su Reglamento de Arbitraje vigente a la fecha de presentación de la solicitud de arbitraje. El Tribunal Arbitral que se designe a tal efecto estará compuesto por un único árbitro y la sede del arbitraje y derecho sustantivo aplicables a la solución de la controversia, serán los correspondientes al domicilio del TACED, http://www.taced.es

12. Procedimiento de revisión y modificaciones

El proceso de revisión de esta política tiene una periodicidad mínima anual, y siempre que se produzca alguna novedad que requiera su revisión.

Se realizará una modificación de este documento siempre que esté justificada desde el punto de vista técnico y legal. Se aplica un control de versionado del documento, especificando fecha de aprobación y publicación, siendo vigente desde el momento de su publicación.

Se establece un control de modificaciones, para garantizar, en todo caso, que las especificaciones resultantes cumplan los requisitos que se pretenden cubrir, que ocasionaron el cambio, y que estén en harmonía con la DPC y adenda de ANF AC.

Se establecen las implicaciones que el cambio de especificaciones tiene sobre las partes que confían, y se prevé la necesidad de notificar dichas modificaciones.

12.1. Procedimiento de publicación y notificación

Esta política, la declaración de prácticas de certificación y adenda de ANF AC, está publicada y permanentemente actualizada, junto con su historial de revisiones, en el sitio web,

https://www.anf.es/repositorio-legal/

12.2. Procedimiento de aprobación de la política

Los miembros de la Junta Rectora de la PKI son los competentes para acordar la aprobación de la presente política.

13. Capacidad financiera

13.1. Indemnización a terceros que confían en el servicio

ANF AC dispone de recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, no obstante, su responsabilidad en el ejercicio de la actividad de PCSC tal como se define en la ETSI EN 319 401 art. 7.1.1.c, queda garantizada mediante un Seguro de Responsabilidad Civil Profesional con una cobertura de,

CINCO MILLONES DE EUROS (5.000.000 €)

13.2. Relaciones fiduciarias

ANF AC no se desempeña como agente fiduciario ni representante en forma alguna de suscriptores ni de terceros que confían en la prestación de sus servicios de confianza.

13.3. Auditorias

ANF AC garantiza la realización de auditorías periódicas de los procesos y procedimientos establecidos. Estas auditorías se llevarán a cabo tanto de manera interna como por auditores independientes acreditados oficialmente para la realización de auditorías de conformidad eIDAS.