Política del Servicio Cualificado de Entrega Electrónica Certificada

Paseo de la Castellana, 79 – 28046 - Madrid (España)
Teléfono: 902 902 172 (llamadas desde España)
Internacional (+34) 933 935 946
Web: www.anf.es

Nivel de Seguridad

Público

Aviso Importante

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

Teléfono: 902 902 172 (llamadas desde España) Internacional (+34) 933 935 946

Web: www.anf.es

Nombre del documento e identificación *(sección 1.2)*

Nombre del documento	Política del Servicio Cualificado de Entrega Electrónica Certificada		
Nombre del archivo	Política QERDS v.1.2.pdf		
Versión	1.1		
Estado de la política	Vigente		
OID	1.3.6.1.4.1.18332.60		
Fecha de aprobación	04/12/2020	**Autor**	F. Díaz Vilches

El identificador de esta Política de Certificación solo será cambiado si se producen cambios sustanciales que afectan a su aplicabilidad.

Revisión y aprobación		
Revisado por	Pablo Díaz	04/12/2020
Aprobado por	MariCarmen Mateo	04/12/2020

Histórico de cambios			
Versión	**Fecha**	**Descripción de la causa**	**Responsable**
1.0	15/01/2020	Nueva Política del Servicio Cualificado de Entrega Electrónica Certificada.	F. Díaz
1.1	01/10/2020	Inclusión referencias a ETSI EN 319 521	F. Díaz
1.2.	04/12/2020	Revisión tras auditoría.	F. Díaz

Índice

Nombre del documento e identificación *(sección 1.2)* **3**

1. Introducción **7**

1.1. Descripción de los servicios 8

1.1.1. Servicio ERDS 9

1.1.2. Servicio QERDS 10

1.1.3. Identificadores cada modalidad de servicio 10

1.2. Nombre del documento e identificación 11

1.3. Partes de la PKI 11

1.4. Ámbito de aplicación 11

1.4.1. Usos permitidos 11

1.4.2. Límites de uso 12

1.4.3. Usos prohibidos 12

1.5. Datos de contacto de la Entidad de Certificación 12

2. Definiciones y Acrónimos **13**

3. Repositorios y publicación de la información **16**

3.1. Repositorios 16

3.2. Publicación de la información 16

3.3. Frecuencia de actualizaciones 16

3.4. Controles de acceso a los repositorios 16

4. Requisitos operacionales **17**

5. Roles de confianza, controles de seguridad física, instalaciones, gestión y operacionales **18**

5.1. Controles de seguridad física y ambiental 18

5.2. Controles operativa 18

5.3. Controles de personal 18

5.4. Seguridad de la red 20

6. Usuarios finales **21**

6.1. Ordenante 21

6.2. Suscriptor 21

6.3. Destinatario 21

6.4. Tercero de confianza 21

7. Identificación y autenticación 22
7.1. Identificación inicial 22
7.2. Autenticación 23

8. Eventos, evidencias y documento probatorio 24
8.1. Frecuencia de procesado 25
8.2. Periodo de retención 25
8.3. Limitaciones al periodo de validez 26
8.4. Protección 26
8.5. Eventos registrados por el servicio 27
8.5.1. Eventos del ERDS origen 27
8.5.1.1 Aceptación de la orden de entrega certificada 27
8.5.2. Eventos de re-transmisión entre ERDS 27
8.5.3. Eventos de aceptación/rechazo por el destinatario 28
8.5.4. Eventos de aceptación/rechazo por el destinatario 30
8.5.5. Eventos de entrega al destinatario 31
8.5.6. Eventos de conexión con sistemas no ERDS 31
8.5.7. Adhesión del destinatario al contenido del documento electrónico 32

9. Obligaciones y responsabilidades 34
9.1. Obligaciones del prestador del servicio 34
9.1.1. Responsabilidad financiera 35
9.1.2. Exoneración de responsabilidad 35
9.2. Obligaciones del emisor y del receptor 36
9.3. Obligaciones de terceras partes que confían 36

10. Cese del servicio QERDS 37
10.1. Acciones previas al cese de la actividad 37
10.1.1. Comunicación a interesados y terceras partes 37
10.1.2. Notificaciones al Organismo de Supervisión 37

11. Limitaciones de responsabilidad 39
11.1. Garantías y limitaciones de garantías 39
11.2. Deslinde de responsabilidades 39

12. Términos y condiciones 40

13. Procedimiento de revisión y modificaciones 43
13.1. Procedimiento de publicación y notificación 43
13.2. Procedimiento de aprobación de la política 43

14. Capacidad financiera 44
14.1. Indemnización a terceros que confían en el servicio 44
14.2. Relaciones fiduciarias 44
14.3. Auditorías 44

15. Resolución de conflictos 45
15.1. Resolución extrajudicial de conflictos 45
15.2. Jurisdicción competente 45

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 OID's 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] 910/2014 del Parlamento Europeo, y con la Ley 59/2003 de Firma Electrónica 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 EN 319 531** *"Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Registered Electronic - Mail Service Providers";* **ETSI EN 319 532** *"Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Registered Electronic - Mail Service Providers".*

ANF AC, emplea las técnicas criptográficas indicadas en la norma TS 119 312. 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.

ANF AC es prestador del "Servicio Cualificado de Entrega Electrónica Certificada" (QeRDS) previsto en el artículo 44 del Reglamento eIDAS (UE) Nº 910/2014 del Parlamento Europeo y del Consejo del 23 de Julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

El presente documento es la **Política del Servicio Cualificado de Entrega Electrónica Certificada** 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.

Este documento 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 de los servicios en cualquiera de los

canales de comunicación disponibles en cada momento, correo electrónico u otros disponibles que permitan una comunicación ERDS:

- Servicio de entrega electrónica certificada.
- Servicios relativos a la entrega electrónica certificada.
  - Identificación de emisor y receptor.
  - Captura de evidencias y elaboración de documento probatorio.
  - Registro y archivo de documentos electrónicos.

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 de Certificación asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; 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 de los servicios

El Servicio de Entrega Electrónica certificada (ERDS) es un servicio que permite la transmisión de datos entre el remitente y los destinatarios por medios electrónicos, proporciona pruebas relativas al manejo de los datos transmitidos, incluida la prueba del envío y recepción de los datos, y que protege los datos transmitidos contra el riesgo de pérdida, robo, daño o cualquier alteración no autorizada.

El canal de comunicación empleado para realizar la entrega al buzón del destinatario puede ser correo electrónico (REM) u otro, siempre que garantice los requerimientos establecidos para ser considerado ERDS.

Para el envío y recepción de mensajes, recogida de evidencias y documentos probatorios, los usuarios disponen de una aplicación / agente de usuario de ERD que está disponible en dos modalidades:

- Plataforma Web Sign to Sign.
- API Sign to Sign.

Mediante esta aplicación todos los usuarios que dispongan de un terminal informático o un SmartPhone, son compatibles para enviar o recibir mensajes certificados en cualquiera de sus modalidades.

Las pruebas consisten en las evidencias de que han sido obtenidas durante la realización del servicio, estas evidencias y el resultado de la transacción quedan recogidas en un documento probatorio. Este documento

probatorio es una declaración formal en la que consta la intervención de ANF AC como parte intermediaria de confianza en la recepción del mandato de entrega recibido del ordenante y su entrega al destinatario, en esta declaración consta el documento electrónico recibido y transmitido, identidad del ordenante y del destinatario, así como todos los eventos que se han generado durante el proceso de envío (evidencia de la orden de entrega por parte del ordenante, trazas de auditoría de los sistemas de comunicaciones, remisión de un mensaje, transmisión de un mensaje, entrega de un mensaje, rechazo de un mensaje, evidencia de entrega al destinatario, canal de comunicación empleado, etc.) especificando el momento determinado en que ocurrió cada evento y el resultado obtenido. El documento probatorio establece la modalidad de servicio prestado y queda autenticado mediante sello electrónico de ANF AC.

En cuanto a la funcionalidad estilo S & N en la plataforma de entrega certificada de ANF AC:

- El servicio permite el estilo S & N dentro de su plataforma, pero no lo permite a mensajes transmitidos por otro ERDS (REMS).
- La aplicación / agente de usuario, dispone de procedimiento para que el usuario pueda aceptar o rechazar un mensaje entrante S & N, y se ofrece información de ayuda para su uso.
- La aplicación ofrece al destinatario la posibilidad de establecer un plazo determinado para aceptación o rechazo de mensajes S & N, y se informa al destinatario del plazo.

ANF AC dispone y ofrece dos modalidades de servicio:

- Servicio ERDS
- Servicio QERDS

El servicio de correo electrónico certificado REMS y QREMS, forma parte de este servicio con la única diferencia de:

- utilizar el protocolo de transferencia SMTP (correo electrónico),
- ofrecer la opción a todos los usuarios de enviar y recibir mensajes en formato MIME según RFC 2045 e RFC 5322, y
- recibir mensajes a través de IMAP o POP.
- Se admite el estilo de operación S&F y S&N.

1.1.1. Servicio ERDS

Un "Servicio de Entrega Electrónica Certificada (ERDS en adelante)" (en inglés, *Electronic Registered Delivery Service*, ERDS) garantiza la entrega segura y confiable de mensajes electrónicos entre las partes, lo que genera evidencia del proceso de envío y entrega a efectos legales.

El nivel de seguridad en la identificación y de intervención de las partes es:

Nivel medio/sustancial:

Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para la mayoría de aplicaciones. Es apropiado para acceder a aplicaciones clasificadas según el ENS en los niveles de Integridad y Autenticidad como de riesgo bajo o medio.

Asimismo, el riesgo previsto por este nivel corresponde a los niveles de seguridad bajo y sustancial de los sistemas de identificación electrónica del reglamento UE 910/2014. Los niveles de seguridad del reglamento eIDAS aplican únicamente a los sistemas de identificación electrónica.

ANF AC interviene en calidad de proveedor de servicios de entrega electrónica certificada (ERDSP).

1.1.2. Servicio QERDS

El Reglamento eIDAS define el llamado Servicio Cualificado de Entrega Electrónica Certificada (en inglés, Qualified Electronic Registered Delivery Service, QERDS), que es un tipo especial de ERDS, en el que tanto el servicio como su prestador deben cumplir una serie de requisitos adicionales respecto a los ERDS convencionales y las entidades que los prestan.

El nivel de seguridad en la identificación y de intervención de las partes es:

Nivel alto:

Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para las aplicaciones que precisan medidas adicionales, en atención al análisis de riesgo realizado. El riesgo previsto por este nivel corresponde al nivel 4 de garantía previsto en la Política Básica de Autenticación de IDABC. Es apropiado para acceder a aplicaciones clasificadas según el ENS en los niveles de Integridad y Autenticidad como de riesgo alto.

Asimismo, el riesgo previsto por este nivel corresponde al nivel seguridad alto de los sistemas de identificación electrónica del reglamento UE 910/2014. Los niveles de seguridad del reglamento eIDAS aplican únicamente a los sistemas de identificación electrónica.

Los mecanismos de seguridad aceptables para todas las partes son certificados cualificados de firma electrónica, y aquellos que ofrezcan el nivel alto de seguridad requerido.

1.1.3. Identificadores cada modalidad de servicio

Con el objeto de identificar los servicios de entrega certificada, ANF AC les ha asignado los siguientes identificadores de objeto (OID).

ERDS	1.3.6.1.4.1.18332.60.1
QERDS	1.3.6.1.4.1.18332.60.2

1.2. Nombre del documento e identificación

Política del Servicio Cualificado de Entrega Electrónica Certificada
OID 1.3.6.1.4.1.18332.60

1.3. Partes que intervienen

- Proveedor de servicios de entrega electrónica certificada (ERDSP): proveedor de servicios de confianza que proporciona un servicio de entrega electrónica registrada, en este caso ANF AC.
- Suscriptor. Corresponde al cliente que contrata el servicio de entrega certificada actúa como ordenante, remitente de la comunicación.
- Usuario. Aplicación o ser humano que interactúa con un cliente de entrega certificada.
- Tercero que confía. Terceros que, sin ser el suscriptor o el usuario, generalmente destinatarios, aunque también pueden ser autores, o peritos judiciales, o Tribunales de Justicia, están autorizados a acceder al mensaje enviado.

1.4. Ámbito de aplicación

1.4.1. Usos permitidos

El uso del Servicio Cualificado de Entrega Electrónica Certificada proporciona las siguientes garantías:

- No repudio de origen y destino

Asegura que el documento proviene del ordenante de quien dice proceder, y se dirige al destinatario al que se debe remitir. Esta característica se obtiene mediante el proceso de

- identificación del ordenante /suscriptor, y
- del destinatario por medio de los procedimientos establecidos en el apartado 7 "Identificación y autenticación de este documento". De esta forma garantiza que el documento proviene de un determinado sujeto debidamente identificado y se dirige a un destinatario cuya identidad ha sido igualmente validada.
- Integridad

Con el empleo del Certificado cualificado de Firma Electrónica o de certificado cualificado de Sello Electrónico, se permite comprobar que el documento no ha sido modificado. Para garantizar la integridad, se utilizan las conocidas funciones resumen (hash), que se utilizan siempre que se realiza una firma o sello electrónico. El uso de este sistema permite comprobar que un mensaje firmado o sellado no ha sido alterado entre el envío y la recepción.

1.4.2. Límites de uso

De forma general, según lo establecido en la DPC de ANF AC, y de forma específica:

- Las comunicaciones y documentos cuya entrega solicita el ordenante deben ser conformes con la legalidad vigente.
- El ordenante tiene la capacidad legal de establecer una comunicación con el destinatario.

1.4.3. Usos prohibidos

De forma general, según lo establecido en la DPC de ANF AC, y de forma específica:

- Las entregas realizadas se ejecutarán únicamente conforme a la función y finalidad que tengan establecida en la presente Política del Servicio Cualificado de Entrega Electrónica Certificada, y con arreglo a la normativa vigente.

- La contratación del servicio admite solamente el uso del servicio en el ámbito de actividad del cliente que contrata el servicio o de la entidad a la que está vinculado, de acuerdo con la finalidad del servicio. El cliente no podrá, salvo acuerdo específico con ANF AC, hacer uso del servicio con fines comerciales del mismo. Se entiende por uso comercial del servicio, cualquier actuación mediante la cual el cliente ofrece a terceras partes ajenas al titular suscriptor, a título oneroso o gratuito, el uso de este servicio de entrega electrónica certificada.

1.5. Datos de contacto de la Entidad de Certificación

Según lo definido en la DPC de ANF AC.

2. 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,

Definiciones

- **Aplicación / agente de usuario de ERD**: sistema que consta de componentes de software y / o hardware mediante el cual los remitentes y los destinatarios participan en el intercambio de datos. En el ámbito de este ERDS, la aplicación es Sign to Sign Derlivery Services.
- **Destinatario**: es la persona física o jurídica a la que se dirige el contenido del ordenante remitente.
- **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.
- **Documento probatorio:** documento que incorpora toda la información relativa a la orden de entrega, evidencias que se han generado y momento en el tiempo en que se han producido. El documento es autenticado por ANF AC mediante sello electrónico de larga vigencia.
- **Evidencias**: son los eventos que se han producido durante la prestación del servicio de entrega certificada, la parte interviniente y el momento en que se ha producido.
- **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 creada 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. En el ámbito de este ERDS la firma electrónica avanzada siempre se genera utilizando un certificado electrónico cualificado vigente.
- **Orden de entrega:** son los datos originales que el Ordenante comunica al ERDSP para solicitar la prestación del servicio.
- **Ordenante:** es la persona física que ordena la entrega electrónica certificada al prestador de servicios y establece los requerimientos para realizar la entrega. El ordenante puede intervenir en su propio nombre y representación, en cuyo caso asume el rol de titular suscriptor del servicio (remitente), o puede intervenir en representación de tercero.
- **Prestador de Servicios de Entrega Electrónica Certificada**: es el proveedor de servicios de entrega electrónica certificada (ERDSP). En algunos escenarios de uso, los ERDSP pueden cooperar

en la transferencia de datos de un remitente a un destinatario cuando están suscritos a diferentes ERDSP. Ver modelos de 4 esquinas y extendidos en las cláusulas 4.3 y 4.4 de ETSI EN 319 522-1 [i.6].

- **Prestador Cualificado de Servicios de Entrega Electrónica Certificada**: es el proveedor QERDSP que está calificado, según se especifica en el Reglamento (UE) nº 910/2014, para la prestación de servicios cualificados de entrega electrónica certificada (QERDS). En el contexto de esta política ANF AC asume este rol.
- **Suscriptor:** es la persona física o jurídica titular remitente de la entrega electrónica certificada (ERD).
- **Transferencia**: acto de hacer que el documento electrónico del ordenante cruce con éxito la frontera de la entrega electrónica registrada del destinatario.
- **Trazas de auditoría:** Son evidencias generadas por los sistemas automatizados que intervienen durante la prestación del servicio, determinan el sistema que ha intervenido y el momento en que intervino.
- **Destinatario:** Persona física o jurídica a la que se dirige la comunicación del ordenante mediante el servicio de entrega certificada.

Acrónimos

- **2FA**: Doble Factor de Autenticación (multifactor)
- **SCA:** Autenticación reforzada de clientes *(Strong Customer Authentication).*
- **ERD**: Entrega electrónica certificada.
- **ERDS**: Servicio de entrega electrónica certificada.
- **ERDSP**: Proveedor de servicios de entrega electrónica certificada.
- **QERDS**: Servicio cualificado de entrega electrónica certificada.
- **QERDSP**: Prestador cualificado de servicio de entrega electrónica certificada.
- **REM**: Correo electrónico registrado.
- **REMS**: Servicio de correo electrónico registrado.
- **QREMS**: Servicio de correo electrónico registrado cualificado.
- **QREMSP**: Proveedor de servicios de correo electrónico registrado.
- **OTP:** One-Time-Password
- **PKI:** Infraestructura de clave pública.
- **SSL:** Capa de puertos seguros. Son protocolos criptográficos que proporcionan comunicaciones seguras por una red y autentican el servidor que presta servicio.
- **S&F:** Almacenamiento y reenvío
- **S&N:** Almacenar y notificar
- **SMTP:** Protocolo simple de transferencia de correo
- **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.

- **QTSP**: Prestador Cualificado de Servicios de Confianza.

3. Repositorios y publicación de la información

3.1. Repositorios

Según lo definido en la DPC de ANF AC.

3.2. Publicación de la información

Según lo definido en la DPC de ANF AC.

3.3. Frecuencia de actualizaciones

Según lo definido en la DPC de ANF AC.

3.4. Controles de acceso a los repositorios

Según lo definido en la DPC de ANF AC.

4. Requisitos operacionales

ANF AC, garantiza que,

- Utiliza un Sistema de Gestión de Seguridad de la Información (SGSI) certificado en 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.
- La presente política se define para el Servicio Cualificado de Entrega Electrónica Certificada, tal y como determina el Reglamento (UE) 910/2014 [2].
- La presente política es conforme a la norma ETSI EN 319 521 "*Policy and security requirements for Electronic Registered Delivery Service Providers*", y ETSI EN 319 522 "*Electronic Signatures and Infrastructures (ESI) Electronic Registered Delivery Services*".

5. Roles de confianza, controles de seguridad física, instalaciones, gestión y operacionales

5.1. Controles de seguridad física y ambiental

Según lo definido en la DPC de ANF AC.

5.2. Controles operativa

Según lo definido en la DPC de ANF AC.

5.3. Controles de personal

Según lo definido en la DPC de ANF AC, y específicamente para el ERDS:

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 siguiendo la política de personal de ANF AC.

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 ordenante y destinatario, en conformidad con lo establecido en esta política y en la DPC de ANF AC.
- **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 autentican 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 acceso es 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 logs de los sistemas de ANF AC.
  Los logs los verá a través de la interfaz web que ofrece la CA. Se utiliza certificado de firma electrónica para control de acceso.
  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 de:
    - Constatar la existencia de toda la documentación requerida y enumerada
    - Comprobar la coherencia de la documentación con los procedimientos, activos inventariados, etc.

ANF AC mantiene los siguientes criterios en relación a la información disponible para auditorías y análisis de incidentes que pueda haber con los certificados.

- **Control y Detección de Incidentes**

  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.

- **Registro de Incidentes**
  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.

5.4. Seguridad de la red

Según lo definido en la DPC de ANF AC.

6. Usuarios finales

Los usuarios finales del servicio son las personas físicas o jurídicas que tienen capacidad para solicitar y obtener la prestación del servicio en las condiciones que se establecen en la presente política.

A los efectos de la presente política, son usuarios finales:

- Ordenante
- Suscriptor
- Destinatario
- Terceros de confianza

6.1. Ordenante

Es la persona física que, en nombre propio o en representación de tercero, y previa identificación, solicita la prestación del servicio. En el supuesto de tratarse de un ordenante que intervienen en nombre de tercero, deberá acreditar su capacidad legal de representación.

6.2. Suscriptor

Es la persona física o jurídica cliente de ANF AC que tiene la consideración de suscriptor, y a cuyo nombre y responsabilidad se presta el servicio como remitente de la comunicación.

6.3. Destinatario

Es la persona física o jurídica a la que el ordenante solicita que le sea entregado un documento electrónico.

6.4. Tercero de confianza

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 DPC de ANF AC.

7. Identificación y autenticación

Todos los requisitos establecidos en este apartado se aplican al servicio REM, toda referencia a ERD, ERDS, o ERDSP, se deberá entender extendida a REM, REMS y REMSP respectivamente.

7.1. Identificación inicial

En el servicio QERDS, la identidad del ordenante y del destinatario se verificará por uno de los medios de identificación de nivel de seguridad sustancial o nivel de seguridad alto *(Art. 8.2 b) y c) del Reglamento eIDAS)* 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.

En el servicio ERDS, la identidad del ordenante y del destinatario se verificará por uno de los medios de identificación de nivel de seguridad bajo (*Art. 8.2.a) del Reglamento eIDAS).*

En el caso de que el ordenante o el destinatario no haya vinculado su identidad a un medio de autenticación, la verificación de identidad se llevará a cabo cada vez que se envíe o entregue un contenido.

En el caso de entrega de SMS, nivel de seguridad bajo (ERDS), la ley española obliga a los Operadores de Telecomunicaciones a realizar una identificación fuerte y completa del propietario de la línea telefónica y/o de datos, con arreglo a las siguientes normas:

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones *(https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950)*
- Ley 25/2007, de 18 de octubre, de conservación de datos relativa a las comunicaciones electrónicas ya las redes públicas de comunicaciones. *(https://www.boe.es/buscar/act.php?id=BOE-A- 2007-18243)*

ANF AC se basa en la identificación realizada por el Operador de telefonía. El Responsable de Identificación podrá solicitar la documentación que considere oportuna para validar esa identificación *(por ej., contrato de línea, facturas, certificado del Operador de Telecomunicaciones, etc.)*

Además, el Ordenante, según se recoge en la cláusula 2ª del contrato de suscripción del servicio *("Contrato S2S")*, con carácter previo, debe haber identificado al destinatario de las operaciones de entrega certificada, en razón de una relación preexistente entre ambos, formalizando por escrito un documento que recoja el consentimiento del destinatario sobre las comunicaciones y asignación de los medios empleados, con mención expresa de los buzones de confianza del destinatario, que éste mantiene bajo su exclusivo control, ya sean números telefonía móvil, direcciones de correo electrónicos u otros.

7.2. Autenticación

En todas las modalidades del Servicio Cualificado de Entrega Electrónica Certificada, se podrá emplear un certificado cualificado de firma o sello electrónico.

Adicionalmente, se podrán emplear mecanismos de autenticación 2FA basados en contraseñas de sesión de un solo uso u OTP (One-Time Password).

El proceso de autenticación utilizando mecanismos 2FA consiste en:

- Envío de una contraseña de sesión de un solo uso utilizando uno de los canales correspondientes al buzón del interesado: SMS, WhatsApp, Mensajería Instantánea, etc.
- Registro de la contraseña de sesión en una aplicación de autenticación multifactor.
- Acceso a la plataforma del servicio mediante usuario y contraseña, y la aplicación de autenticación multifactor empleada.

El proceso de autenticación utilizando mecanismos OTP consiste en:

- Envío de un código QR por email a la identificación de correo electrónico.
- Registro del código QR en una aplicación de autenticación multifactor.
- Acceso a la plataforma del servicio mediante usuario y contraseña, y la aplicación de autenticación multifactor empleada.

El ordenante establece los requerimientos de identificación y autenticación que deben ser contemplados por el ERDS, los requerimientos determinan la modalidad ERDS o QERDS.

8. Eventos, evidencias y documento probatorio

ANF AC, mantendrá un registro de los eventos del servicio mediante logs y trazas de auditoría que se pueden consultar directamente desde la aplicación.

Todos los requisitos establecidos en este apartado se aplican al servicio REM, toda referencia a ERD, ERDS, o ERDSP, se deberá entender extendida a REM, REMS y REMSP respectivamente.

Cada servicio ERDS cuenta con un identificador único.

Todas las evidencias producidas por el servicio se pueden descargar en formato PDF. Cada evidencia cuenta con un identificador único de evidencia, incluye identificador ERDS, y detalla información de la identidad del ordenante y del destinatario, sistemas automatizados que en su caso han intervenido, información relativa a eventos, momento en que se han producido y trazas de auditoría que se han obtenido.

Cada evidencia está autenticada mediante sello electrónico de ANF AC que incluye comprobación OCSP y sello cualificado de tiempo electrónico que cumple los estándares XAdES, ETSI TS 10317, v.2.1.1, (nivel LT y LTA) de acuerdo con la Decisión de Implementación (UE) 2015 / 1506 de la Comisión de 8 de septiembre de 2015, por la que se establecen especificaciones para formatos avanzados de firma electrónica y sellos electrónicos avanzados del Reglamento (UE) nº 910/2014.

El conjunto de evidencias generadas en cada servicio de entrega electrónica certificada es recopilado en un único documento PDF denominado "Documento Probatorio". Este documento cuenta con un identificador único de evidencia, incluye identificador ERDS, en el que consta modalidad de servicio, el resultado final del servicio realizado, y detalla información del conjunto de las evidencias generadas.

El documento probatorio está autenticado mediante sello electrónico de ANF AC que incluye comprobación OCSP y sello cualificado de tiempo electrónico que cumple los estándares XAdES, ETSI TS 10317, v.2.1.1, (nivel LT y LTA) de acuerdo con la Decisión de Implementación (UE) 2015 / 1506 de la Comisión de 8 de septiembre de 2015, por la que se establecen especificaciones para formatos avanzados de firmas electrónicas y sellos electrónicos avanzados del Reglamento (UE) nº 910/2014.

Para la obtención de pruebas relacionadas de los datos transmitidos, la aplicación ERD dispone de un sistema que permite obtener copia autenticada de las evidencias y documento probatorio de la transmisión realizada. La aplicación ERD requiere, previo al acceso, identificación del usuario que como mínimo será de nivel de seguridad sustancial. Así mismo, ANF AC ofrece la posibilidad de solicitar copia autenticada por alguno de los siguientes procedimientos:

- Personación en las oficinas administrativas de ANF AC,
  Gran Vía de les Corts Catalanes, 996 piso 3 y 4

08018 – Barcelona - España

acreditando identidad mediante documento legal (DNI, Pasaporte, tarjeta de residencia), en caso de representación de tercero mediante poder notarial.

- Correo postal remitido a las oficinas administrativas de ANF AC, se incluirá acreditación de identidad.

Las pruebas relacionadas de los datos transmitidos solo son accesibles:

- Al ordenante.
- Al suscriptor titular remitente.
- Al destinatario siempre que la entrega electrónica certificada se hubiera realizado de forma efectiva.
- Por mandamiento judicial.

Si la identificación del destinatario se basa en una firma electrónica avanzada o cualificada, y la validación de la firma está en conformidad, se procederá a la notificación al destinatario sin otros requerimientos de control de autenticación.

8.1. Frecuencia de procesado

Los registros de auditoría se examinan periódicamente en búsqueda de actividad sospechosa o no habitual.

8.2. Periodo de retención

ANF AC custodia durante el período legal nacional aplicable después de la fecha de envío, toda la evidencia relevante. Como mínimo mantiene en línea todos los registros de la información transmitida por un periodo mínimo de 6 meses, y durante un periodo de hasta 15 años en backup.

La información preservada será, como mínimo:

a) datos de identificación de los usuarios;

b) datos de autenticación de usuarios;

c) prueba de la verificación inicial de la identidad del remitente;

d) registros de la operación del ERDS, verificación de identidad del remitente y destinatario y comunicación;

e) prueba de la verificación de la identidad del destinatario antes del envío / entrega del contenido del usuario;

f) medios para demostrar que el contenido del usuario no ha sido modificado durante la transmisión;

g) una referencia o un resumen del contenido completo del usuario enviado; y

h) fichas de sello de tiempo correspondientes a la fecha y hora de envío, consignación y entrega y modificación del contenido del usuario, según corresponda.

8.3. Limitaciones al periodo de validez

ANF AC garantizará la validez de las evidencias y documentos probatorios durante todo el periodo de retención.

8.4. 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 en un dispositivo 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 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).

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

El ordenante firma la notificación quedando garantizada autenticidad de origen e integridad de contenido. El ERDS, previo a aceptar la notificación, realiza verificación de firma, y previo a la transmisión al destinatario se procede a verificar las firmas que autentican la notificación.

Todo el proceso de identificación se realiza en un entorno seguro y controlado de acuerdo con las medidas de seguridad fisica y logica establecidas en la DPC y adenda de ANF AC. ANF AC garantiza la confidencialidad, integridad y disponibilidad de los registros.

8.5. Eventos registrados por el servicio

8.5.1. Eventos del ERDS origen

8.5.1.1 Aceptación de la orden de entrega certificada

El ordenante se ha identificado, interviniendo en su nombre en calidad de titular suscriptor o en representación de un tercero, y ha transmitido al servicio de entrega certificada una solicitud de comunicación con especificación de los requerimientos de entrega.

ANF AC, ha verificado la solicitud y ha aceptado el encargo de entrega certificada.

La evidencia atestigua la identidad del ordenante y del suscriptor, que debidamente autenticado de acuerdo con los detalles indicados en la evidencia, ha transmitido con éxito, en el momento indicado en la evidencia en sí, la identidad de uno o varios destinatarios, el canal de comunicación a emplear para realizar la entrega certificada, un contenido a poner a disposición del destinatario, requerimientos que el ordenante establece para hacer efectiva la entrega (p.ej. certificado de firma electrónica, 2FA y/o confirmación de lectura), y aceptación por parte de ANF AC de la orden de entrega y momento en el que se acepta la orden.

8.5.1.2 Denegación de la prestación del servicio

La entrega electrónica certificada solicitada por el ordenante, no fue aceptada por el ERDS. El prestador del servicio puede rechazar una solicitud siempre que lo considere oportuno, ya sea por razones políticas, comerciales, formales o técnicas.

La evidencia relacionada con la denegación de servicio atestigua se ha rechazado la prestación del servicio al ordenante, y el momento en el que se produce el rechazo.

8.5.2. Eventos de re-transmisión entre ERDS

8.5.2.1 Aceptación de la re-transmisión

Un mensaje ERD enviado por el ERDS de retransmisión y recibido con éxito por el ERDS retransmitido, fue aceptado por este último.

La evidencia relacionada atestigua que, en situaciones donde varios ERDS están cooperando para ofrecer conjuntamente el servicio ERD, un ERDS intermedio o del destinatario ha aceptado un mensaje ERD enviado por el ERDS anterior en la cadena antes mencionada.

8.5.2.2 Rechazo de la re-transmisión

Un mensaje de ERD enviado por la retransmisión ERDS y recibido con éxito por la retransmisión ERDS, fue rechazado por la última debido a razones políticas, formales o técnicas.

La evidencia relacionada atestigua que, en situaciones donde varios ERDS están cooperando para ofrecer conjuntamente el servicio ERD, un ERDS intermedio o del destinatario, en el momento especificado por la evidencia, ha rechazado un mensaje de ERD emitido por el ERDS anterior en el caso mencionado anteriormente.

8.5.2.3 Fallo de la re-transmisión

No fue posible retransmitir en un período de tiempo determinado un mensaje de ERD al ERDS destino debido a errores técnicos u otros problemas. Por ejemplo: la imposibilidad de identificar el ERDS destino, el ERDS destino es inalcanzable o el ERDS destino rechazó la comunicación sin proporcionar una razón.

La evidencia relacionada atestigua que, en el momento especificado en la evidencia, fue imposible enviar un mensaje ERD dentro de un período de tiempo dado a un proveedor intermedio de ERDS o al proveedor de ERDS del destinatario debido a errores técnicos y / u otros problemas.

8.5.3. Eventos de aceptación/rechazo por el destinatario

8.5.3.1 Notificación para la aceptación

El sistema que administra la cuenta del destinatario, confirma que depositó en la cuenta del destinatario una comunicación del ERDS notificando al destinatario sobre la disponibilidad de un mensaje (sin divulgar necesariamente su remitente, contenido, etc.) y solicitando la disposición del destinatario para aceptarlo (p.ej. notificación al destinatario de que le ha sido enviado un documento electrónico y puede recogerlo accediendo a la plataforma de entrega certificada)

La evidencia relacionada atestigua que una notificación solicitando la aceptación de un mensaje ha sido enviada a un destinatario en un momento específico según lo indicado por la evidencia. La evidencia da fe del aviso de entrega enviado al sistema que administra la cuenta del destinatario.

8.5.3.2 Fallo en la notificación para la aceptación

No se pudo notificar al destinatario dentro de un período de tiempo dado debido a errores técnicos y / u otras razones, o no existe ningún comprobante de notificación del sistema que administra la cuenta del destinatario dentro de un período determinado.

El límite de tiempo lo fijan las normas legales o contractuales, o está determinado por la política del ERDS, o ha sido predefinido por el ordenante.

La evidencia relacionada atestigua que una notificación que solicita la aceptación de un mensaje no se pudo enviar al destinatario especificado después de un cierto número de intentos o un tiempo de espera como se especifica en las políticas aplicables.

8.5.3.3 Notificación de la modificación del contenido

El EDRS, no realiza cambios en el contenido facilitado por el ordenante, ni tan siquiera modifica el formato del documento electrónico.

El ERDS, previo a la transmisión del documento electrónico, realiza una comprobación de integridad a fin de detectar cualquier modificación del contenido. En el caso de que la validación sea negativa, no se realiza la transmisión.

La evidencia relacionada atestigua que una notificación que solicita la aceptación de un mensaje no se pudo enviar al destinatario especificado por modificación de la notificación original entregada por el ordenante.

8.5.3.4 Aceptación de la consignación

El destinatario realizó una acción explícita (p.ej. 2FA) indicando al ERDS que emitió la notificación de la aceptación de recibir un documento electrónico.

La evidencia atestigua que el destinatario, con la identificación y autenticación adecuadas, en el momento indicado por la evidencia realizó una acción explícita mediante la que acepta recibir el documento electrónico consignado por el ordenante.

8.5.3.5 Rechazo de la consignación

El destinatario, tras una identificación y autenticación adecuadas, realizó una acción explícita que indica que el destinatario rechazó recibir el documento consignado por el ordenante.

La evidencia relacionada atestigua que el destinatario, con la identificación y autenticación adecuadas, en el momento indicado por la evidencia, rechaza recibir el contenido que el ordenante consignó.

8.5.3.6 Caducidad de la aceptación / rechazo

El ERDS envió una notificación al destinatario, pero no respondió a la notificación con una aceptación / rechazo.

La evidencia relacionada atestigua que el destinatario, en el momento indicado por la evidencia no reaccionó a la solicitud de aceptar / rechazar para recibir algún contenido consignado por el ordenante dentro de un período de tiempo definido.

Este período de tiempo puede determinarse mediante legislación, reglas de política del ERDS, o parámetros dados por el ordenante.

8.5.4. Eventos de aceptación/rechazo por el destinatario

8.5.4.1 Consignación del contenido

El sistema que administra la cuenta del destinatario, confirma que la comunicación transmitida por el ERDS ha sido depositada en su cuenta.

La evidencia relacionada atestigua que, el mensaje de ERD, en un momento específico indicado por la evidencia, se puso a disposición del destinatario.

8.5.4.2 Fallo de consignación del contenido

El contenido consignado por el ordenante no puede estar disponible para el destinatario dentro de un período de tiempo dado debido a errores técnicos y / u otras razones o no existe prueba de entrega dentro de un período determinado.

La evidencia relacionada atestigua que el mensaje ERD no pudo estar disponible para el destinatario dentro de un período de tiempo dado. La emisión de esta evidencia puede ser desencadenada por diferentes eventos, a modo meramente enunciativo, no limitativo:

- El sistema que administra la cuenta del destinatario, no pudo enviar la comunicación a la cuenta del destinatario.
- Un ERDS de retransmisión no recibió, dentro de un período de tiempo dado, del ERDS transmitido una evidencia de envío exitoso. En este caso, es el ERDS de retransmisión el que crea la evidencia con el código de razón adecuado.
- El sistema 2FA no pudo transmitir con éxito el código de verificación o QR al destinatario.
- Fallo técnico de la plataforma de publicación del ERDS.

8.5.4.3 Notificación de consignación

Se envió una notificación al destinatario sobre la disponibilidad del mensaje consignado.

La evidencia relacionada atestigua que se ha enviado una notificación sobre la disponibilidad del mensaje consignado a un destinatario en un momento específico según lo indicado por la evidencia.

8.5.4.4 Fallo de notificación de consignación

Falló un intento de notificar al destinatario sobre la disponibilidad del contenido del usuario.

La evidencia relacionada atestigua que una notificación sobre la disponibilidad del contenido del usuario consignado no pudo ser transmitida.

8.5.5. Eventos de entrega al destinatario

8.5.5.1 Entrega del contenido

El documento electrónico fue entregado al destinatario.

La evidencia relacionada atestigua que el documento electrónico consignado por el ordenante, en un momento específico fue transmitido íntegramente al destinatario.

8.5.5.2 Fallo de entrega del contenido

El documento electrónico no fue entregado al destinatario.

La evidencia relacionada atestigua que el documento electrónico consignado por el ordenante, no fue entregado al destinatario después de un cierto número de intentos o un tiempo de espera especificado por las políticas aplicables.

8.5.5.3 Fallo por imposibilidad de acceso al contenido

El documento electrónico no es accesible al destinatario debido a causas técnicas (p.ej. documento cifrado corrupto, fallo de integridad del documento electrónico, detección de contenido ilícito, etc).

La evidencia relacionada atestigua que el documento electrónico consignado por el ordenante, no es accesible al destinatario por causas técnicas o formales detalladas en la evidencia.

8.5.6. Eventos de conexión con sistemas no ERDS

8.5.6.1 Reenvío a un sistema no ERDS

Se envió un mensaje determinado con éxito a un sistema que no facilita confirmación de recepción.

La evidencia relacionada atestigua que un cierto mensaje ERD fue reenviado exitosamente al sistema que administra la cuenta del destinatario a la hora indicada en la evidencia, pero el sistema no emite confirmación de recepción.

8.5.6.2 Fallo en el reenvío a un sistema no ERDS

El intento de retransmitir un mensaje a un sistema no ERDS falló debido a errores técnicos y / u otras razones.

La evidencia relacionada atestigua que un cierto mensaje ERD no pudo ser reenviado a un sistema no ERDS en el momento indicado en la evidencia.

8.5.6.3 Recepción desde un sistema no ERDS

Se recibió un cierto mensaje de un sistema no ERDS, por lo tanto, no se puede confiar en toda la información relacionada con su envío, como el identificador del remitente y el tiempo de envío.

La evidencia relacionada atestigua que se recibió un determinado mensaje de un sistema externo que no es ERDS, por lo tanto, toda la información sobre el origen del mensaje no es confiable.

8.5.7. Adhesión del destinatario al contenido del documento electrónico

8.5.7.1 Notificación para la adhesión

El ERDS notifica al destinatario que el ordenante solicita una acción explícita que acredite la conformidad del destinatario al contenido del documento electrónico entregado, y procedimiento a seguir.

La evidencia relacionada atestigua que una notificación solicitando la aceptación y adhesión a los términos expresados en el documento electrónico entregado por el ERDS, ha sido solicitada al destinatario en un momento específico y el procedimiento que el destinatario debe realizar en caso de conformidad.

8.5.7.2 Fallo en la notificación para la adhesión

No se pudo notificar al destinatario dentro de un período de tiempo dado debido a errores técnicos y / u otras razones, o no existe ningún comprobante de notificación del sistema que administra la cuenta del destinatario dentro de un período determinado.

El límite de tiempo lo fijan las normas legales o contractuales, o está determinado por la política del ERDS, o ha sido predefinido por el ordenante.

La evidencia relacionada atestigua que la notificación de adhesión no se pudo enviar al destinatario especificado después de un cierto número de intentos o un tiempo de espera como se especifica en las políticas aplicables.

8.5.7.3 Adhesión al documento electrónico

El destinatario realizó una acción explícita (p.ej. firma electrónica, firmagrafo métrica, 2FA, etc) como expresión de su voluntad y consentimiento a aceptar y adherirse a los términos expresados en el documento electrónico entregado por el ERDS y, en caso de ser requerimiento de la transacción, el destinatario realiza un mandato al prestador del ERDS para que, en calidad de mandatario, firme en su nombre la conformidad de aceptación del contenido del documento electrónico.

La evidencia atestigua que el destinatario, con la identificación y autenticación adecuadas, en el momento indicado por la evidencia realizó una acción explícita mediante la que acepta y se adhiere al contenido del documento electrónico consignado por el ordenante y, en su caso, para que el prestador del ERDS en

calidad de mandatario del destinatario (mandante), firme en su nombre la aceptación del documento electrónico.

8.5.7.4 Rechazo a la adhesión del documento electrónico

El destinatario, tras una identificación y autenticación adecuadas, realizó una acción explícita que indica que el destinatario rechazó adherirse a los términos contenidos en el documento consignado por el ordenante.

La evidencia relacionada atestigua que el destinatario, con la identificación y autenticación adecuadas, en el momento indicado por la evidencia, rechaza adherirse a los términos contenidos en el documento consignado por el ordenante.

8.5.7.5 Caducidad de la adhesión / rechazo

El ERDS envió una notificación al destinatario, pero no respondió a la notificación con una adhesión / rechazo.

La evidencia relacionada atestigua que el destinatario, en el momento indicado por la evidencia no reaccionó a la solicitud de adhesión / rechazo para aceptar el contenido del documento electrónico.

Este período de tiempo puede determinarse mediante legislación, reglas de política del ERDS, o parámetros dados por el ordenante.

9. Obligaciones y responsabilidades

9.1. 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 QERDS. Se obliga a:

- Respetar lo dispuesto en esta Política del Servicio Cualificado de Entrega Electrónica Certificada.
- Proteger sus claves privadas de forma segura.
- Prestar el Servicio Cualificado de Entrega Electrónica Certificada según la información enviada por el ordenante y libres de errores de entrada de datos.
- 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 del Servicio Cualificado de Entrega Electrónica Certificada.
- Informar sobre las modificaciones de la Política del Servicio Cualificado de Entrega Electrónica Certificada a clientes y terceros que confían en los servicios.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.
- Custodiar las evidencias emitidas para los clientes que contraten el Servicio Cualificado de Entrega Electrónica Certificada.
- Responder por el incumplimiento de lo establecido en esta Política del Servicio Cualificado de Entrega Electrónica Certificada y, allí donde sea aplicable.
- Utilizar certificado de sello electrónico que identifica el servicio de entrega electrónica certificada y destinarlo a ese único fin.
- Todas las personas que intervienen en la gestión y administración del servicio de entrega electrónica certificada, están obligadas a guardar secreto de toda la información gestionada por ANF AC, habiendo suscrito el correspondiente compromiso de confidencialidad.

- Proteger la confidencialidad de la identidad del remitente y destinatario, o entre componentes distribuidos del sistema ERDS.
- Garantizar la confidencialidad de las comunicaciones, 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.

9.1.1. Responsabilidad financiera

Se aplica dentro de los límites establecidos en la vigente Ley de Firma electrónica. ANF AC no se hace responsable en caso de pérdidas por transacciones.

9.1.2. Exoneración de responsabilidad

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

- Daños causados por ataques externos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en las presentes Políticas de QERDS 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 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 de QERDS.

ANF AC, no revisa los contenidos de las comunicaciones del ordenante, interviene como mero proveedor del servicio de comunicaciones, por tanto, la intervención de ANF AC no puede presuponer adhesión al contenido del mensaje, ni ANF AC es responsable del mismo.

9.2. Obligaciones del emisor y del receptor

- Respetar lo dispuesto en esta Política del Servicio Cualificado de Entrega Electrónica Certificada.
- Proteger sus claves privadas de forma segura.
- Respetar lo dispuesto en los documentos contractuales firmados con ANF AC.
- Reportar cualquier incidente de seguridad tan pronto como este sea identificado.
- No utilizar el servicio ERDS para comunicaciones que están prohibidas por la legislación vigente.
- Utilizar los recursos técnicos del ERDS, de acuerdo con indicaciones establecidas por ANF AC.
- Está prohibido la aplicación de ingeniería inversa y la búsqueda de fallos en la lógica del sistema.
- Garantizar que las órdenes de envío obedecen a una relación jurídica con los destinatarios y que no son comunicaciones no deseadas por los mismos, salvo cuando el envío esté amparado por lo dispuesto en una ley.

9.3. 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 por la Política del Servicio Cualificado de Entrega Electrónica Certificada.
- Reportar cualquier incidente de seguridad tan pronto como este sea identificado.
- Tener en consideración otras precauciones descritas en acuerdos u otros sitios.

10. Cese del servicio QERDS

En caso de cese del Servicio Cualificado de Entrega Electrónica Certificada, se deberán aplicar las siguientes acciones:

10.1. 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.

10.1.1. Comunicación a interesados y terceras partes

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 las partes de confianza, 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.

10.1.2. 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.

10.1.3. 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.

10.1.4. 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.

10.1.5. Transferencia de la gestión del servicio

No se contempla la transferencia de la gestión del servicio.

10.2. 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.

11. Limitaciones de responsabilidad

11.1. Garantías y limitaciones de garantías

ANF AC limita su responsabilidad restringiendo el servicio a la entrega electrónica certificada suministrada.

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.

11.2. Deslinde de responsabilidades

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

- Daños causados por ataques externos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en las presentes Políticas de QERDS 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 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 de QERDS.
- Daños 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.

12. 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 ERDS. Este documento está permanentemente publicado en formato pdf y puede ser descargado en,

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

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.

Constitución de la entrega

El Servicio Cualificado de Entrega Electrónica Certificada proporciona la entrega segura y confiable de mensajes electrónicos entre las partes, produciendo evidencia del proceso de entrega para la responsabilidad legal.

De acuerdo con el artículo 28 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información, el ERDS considera realizada la entrega en el momento en que los sistemas que administran la cuenta del destinatario confirman su recepción.

La entrega generará una evidencia que se almacenará asociada al mensaje en la plataforma y será puesta a disposición del ordenante del servicio.

El ERDS considera que el destinatario ha accedido al documento cuando realiza una acción explícita de conformidad de recogida.

El acceso del destinatario al documento generará una evidencia que se almacenará asociada al mensaje en la plataforma y será puesta a disposición del ordenante del servicio.

La evidencia se elabora como una declaración del Prestador del Servicio de Entrega Electrónica Certificada de que un evento específico, rigurosamente detallado, relacionado con el proceso de entrega ocurrió en un momento determinado. La evidencia se puede entregar inmediatamente al ordenante o puede guardarse en un repositorio para su posterior acceso por parte de partes interesadas.

La evidencia es codificada con un identificador exclusivo y autenticada mediante sello electrónico de larga vigencia de ANF AC, dejando así constancia de la responsabilidad asumida y garantizando su integridad.

Todas las evidencias asociadas a una entrega electrónica certificada, son recopiladas en un documento probatorio.

El documento probatorio es codificado con un identificador exclusivo y autenticado mediante sello electrónico de larga vigencia de ANF AC, dejando así constancia de la responsabilidad asumida y garantizando su integridad.

Disponibilidad de los datos de entrega

Una vez constituida la entrega, el destinatario dispondrá de un plazo máximo establecido por el ordenante para confirmar la recepción de los datos, que en ningún caso será superior a seis meses. Una vez superado este umbral, los datos de la entrega dejarán de estar disponibles para su recepción por parte del destinatario.

Disponibilidad del servicio

El Servicio Cualificado de Entrega Electrónica Certificada 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 de quien lo demanda, con independencia de la rapidez o ritmo al que posteriormente éste sea prestado.

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).

Seguridad del Sistema de Gestión de la Información

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

Términos legales

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

Explícitamente se asumen como de aplicación las siguientes normas:

- Reglamento (UE) n.º 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 (Reglamento eIDAS) y por la que se deroga la Directiva 1999/93/CE.

- 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 Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.
- Ley 59/2003 de firma electrónica.

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

13. 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.

13.1. 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/

13.2. 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.

14. Capacidad financiera

14.1. 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 €)

14.2. 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.

14.3. Auditorías

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.

15. Resolución de conflictos

15.1. Resolución extrajudicial de conflictos

ANF AC se somete formalmente en su declaración de Términos y Condiciones a procedimiento arbitral institucional del Tribunal de Arbitraje TACED.

15.2. Jurisdicción competente

La relación entre ANF AC y las partes que confían se rige exclusivamente por la legislación española.