Servicio Cualificado de Entrega Electrónica Certificada (QERDS)

Declaración de Prácticas

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

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 es Prestador Cualificado de Servicios de Confianza (PCSC) en cumplimiento del Reglamento eIDAS y la legislación nacional vigente.

ANF AC es prestador del "Servicio Cualificado de Entrega Electrónica Certificada" (QERDS) previsto en el artículo 44 del Reglamento (UE) Nº 910/2014[1] 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 (en adelante Reglamento eIDAS), prestado en conformidad con:

- **Ley 6/2020,** de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza,
- **ETSI EN 319 401** *(General Policy Requirements for Trust Service Providers).*
- **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".*

El presente documento es la **Declaración de Prácticas del Servicio Cualificado de Entrega Electrónica Certificada**, que define los requisitos de procedimiento y operacionales a los que está sujeto el uso del servicio, y las prácticas 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 declaración de prácticas está subordinada a la Declaración de Prácticas de Certificación (DPC) de ANF AC. Toda la documentación está a libre disposición de usuarios y terceros que confían en https://www.anf.es/repositorio-legal/.

[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

Esta declaración de prácticas 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. Nombre del documento e identificación

Nombre del documento	Declaración de Prácticas del Servicio Cualificado de Entrega Electrónica Certificada		
Versión	1.5.		
OID	1.3.6.1.4.1.18332.60		
Fecha de aprobación	27/03/2024	**Fecha de publicación**	27/03/2024

1.1.1. Revisiones

El proceso de revisión de esta declaración de prácticas tiene una periodicidad mínima anual, y siempre que se produzca alguna novedad que requiera su revisión y esté justificada desde el punto de vista técnico y legal. La versión sólo será cambiada si se producen cambios sustanciales que afectan a su aplicabilidad.

Los miembros de la Junta Rectora de la PKI son los competentes para acordar la aprobación de la presente declaración de prácticas, garantizando que los cambios cumplan los requisitos que se pretenden cubrir, que estén en harmonía con la DPC y adenda de ANF AC. Previo a la publicación de actualizaciones se valorarán las implicaciones sobre las partes que confían, y se prevé la necesidad de notificar dichas modificaciones por vía de correo electrónico certificado a cada uno de los usuarios, al CAB y al Organismo de Supervisión.

Versión	Cambios	Aprobación	Publicación
1.5.	Cambios menores de redacción y mención a eIDAS 2.	27/03/2024	27/03/2024
1.4.	Revisión annual. Renamed from “Policy” to “Practice Statement” as indicated in ETSI EN 319 521.	14/03/2023	14/03/2023
1.3.	Revisión anual. Clarificación del método de rechazo de orden de Entrega, y del modelo S&N vs. S&F. El servicio ERDS no realiza transmisión a otros ERDS.	15/10/2021	15/10/2021
1.2.	Revisión tras auditoría	04/12/2020	04/12/2020
1.1.	Inclusión referencias a ETSI EN 319 521	01/10/2020	01/10/2020
1.0.	Nueva Política del Servicio Cualificado de Entrega Electrónica Certificada.	15/01/2020	15/01/2020

1.2. Definiciones y Acrónimos

En esta declaración de prácticas aplican las definiciones especificadas en la DPC de ANF AC, además de las siguientes:

Español	Inglés	Acrónimo	Definición
Ordenante	*Sender*		Persona física o jurídica que ordena el envío del contenido del usuario 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 (ordenante), o puede intervenir en representación de tercero.

Destinatario	*Recipient*		Persona física o jurídica a la que se dirige el contenido del usuario.
Contenido de usuario	*user content*		Datos originales producidos por el ordenante que deben ser entregados al destinatario.
Consignación	*consignment*		Acto de poner el contenido de usuario a disposición del destinatario, dentro de los límites del servicio de entrega electrónica certificada.
Transferencia	*handover*		Acto de hacer que el contenido del usuario cruce con éxito la frontera del servicio de entrega electrónica certificada del destinatario hacia el ERD-UA del destinatario.
Servicio de Entrega Electrónica Certificada	*Electronic Registered Delivery Service*	ERDS	Servicio electrónico que permite la transmisión de datos entre el ordenante y los destinatarios por medios electrónicos y proporciona evidencias relacionadas con el 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, daños o alteraciones no autorizadas.
Servicio Cualificado de Entrega Electrónica Certificada	*Qualified Electronic Registered Delivery Service*	QERDS	Como se especifica en el Reglamento eIDAS.
Prestador de Servicio de Entrega Electrónica Certificada	*Electronic Registered Delivery Service Provider*	ERDSP	Prestador de servicios de confianza que proporciona un servicio de entrega electrónica certificada.
Prestador Cualificado de Servicio de Entrega Electrónica Certificada	*Qualified Electronic Registered Delivery Service Provider*	QERDSP	Prestador de servicios de confianza que proporciona servicios cualificados de entrega electrónica certificada.
Aplicación/Agente usuario ERD	*ERD user agent/application*	ERD-UA	Sistema que consta de componentes de software y/o hardware mediante los cuales los ordenantes y los destinatarios participan en el intercambio de datos con los ERDSP. En el ámbito de este ERDS, la aplicación es Sign to Sign Delivery Services.
Evidencia ERDS o Trazas de auditoría	*ERDS evidence*		Datos generados dentro del ERDS, que tiene como objetivo demostrar que un determinado evento ha ocurrido en un momento determinado.
Documento probatorio	*Probative document*		Documento que incorpora toda la información relativa a la transacción, 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.
Declaración de Prácticas ERDS	*ERDS practice statement*		Declaración de las prácticas que emplea un ERDSP para proporcionar sus servicios.

Almacenamiento y Reenvío	*Store and Forward*	S&F	Estilo de funcionamiento de un REMS en el que el contenido de usuario proporcionado por el ordenante se transmite al destinatario por valor, y no se requiere aceptación explícita del destinatario.
Almacenamiento y notificación	*Store and Notify*	S&N	Estilo de funcionamiento de un REMS en el que primero se transmite al destinatario una referencia al contenido del usuario, y se requiere la aceptación del destinatario antes del envío del contenido del usuario en sí.
Correo electrónico certificado	*Registered electronic mail*	REM	Es un tipo específico de entrega electrónica certificada, que se basa en los formatos, protocolos y mecanismos utilizados en la mensajería de correo electrónico ordinaria.

1.3. Datos de contacto del ERDSP

Según lo definido en la DPC de ANF AC.

Departamento	Junta Rectora de la PKI
Correo electrónico	juntapki@anf.es
Dirección	Paseo de la Castellana, 79. 28046, Madrid.
Dirección Administrativa.	Gran Vía de les Corts Catalanes, 996 piso 3 y 4 08018, Barcelona.
Número de teléfono	932 661 614 (desde España) Internacional (+34) 933 935 946

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

Web	https://reportarproblema.anf.es
Correo electrónico	info@anf.es
Personación en oficinas administrativas ANF AC.	Gran Vía de les Corts Catalanes, 996 piso 3 y 4 08018, Barcelona.
Número de teléfono	932 661 614 (desde España) Internacional (+34) 933 935 946

2. Descripción del servicio

2.1. Tipo de servicio según cualificación

2.1.1. Servicio ERDS

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

Este servicio ha sido diseñado y es gestionado en conformidad con las normas ETSI:

- **EN 319 521***: "Policy and security requirements for Electronic Registered Delivery Service Providers";*
- **EN 319 531**: *"Policy and security requirements for Registered Electronic - Mail Service Providers";*

Los datos enviados y recibidos mediante el servicio ERDS tienen efectos legales y no se debe negar su admisibilidad como prueba en procedimientos judiciales únicamente por el hecho de que se encuentren en formato electrónico o que no cumplan con los requisitos del servicio QERDS (sección 2.1.2.).

Con el objeto de identificar los servicios de entrega certificada ERDS, ANF AC ha asignado el siguiente OID **1.3.6.1.4.1.18332.60.1.**

2.1.2. Servicio QERDS

El Reglamento eIDAS establece una serie de requisitos adicionales que tanto el prestador como el servicio deben cumplir respecto a los ERDS convencionales y las entidades que los prestan. Este servicio QERDS es el servicio ERDS (sección 2.1.1.) que aplica los requerimientos adicionales establecidos en el artículo 44 del Reglamento eIDAS. Este servicio ha sido diseñado y es gestionado en conformidad con:

- **Artículo 44** del Reglamento eIDAS.
- **EN 319 521***: "Policy and security requirements for Electronic Registered Delivery Service Providers";*
- **EN 319 531**: *"Policy and security requirements for Registered Electronic - Mail Service Providers";*

Los datos enviados y recibidos mediante el servicio QERDS gozan de la presunción de integridad de los datos, el envío de esos datos por el ordenante identificado, su recepción por el destinatario identificado y la exactitud de la fecha y hora de envío y recepción indicado por el servicio.

Con el objeto de identificar los servicios de entrega certificada cualificada QERDS, ANF AC ha asignado el siguiente OID **1.3.6.1.4.1.18332.60.2.**

Sign to Sign Delivery Services			
Subject	CN = Sign to Sign Delivery Services	**Serial number**	995076565929189897695095607
	OI = VATES-G63287510	**Clave Pública**	RSA (2048 Bits)

	OU = Certificado Cualificado de Sello Electronico		
	O = ANF Autoridad de Certificación	**Algorítmo defirma**	Sha256RSA
	C = ES L=Barcelona, ST=Cataluña		
Periodo de vigencia	Válido desde 2023-02-01 17:06:59 hasta 2025-01-31 17:06:59 2022-12-02 13:52:56		
x509SKI	dWcb0YbrRtAl45eg1GMDPLD0xc0		

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.

2.2. ERD-UA

Para el envío y recepción de comunicaciones, recogida de evidencias y generación de los documentos probatorios, los usuarios disponen de una aplicación (ERD-UA) 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.

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

2.3. Partes que intervienen en el servicio

- **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.
- **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.
- **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 ordenante de la comunicación.
- **Destinatario**: Es la persona física o jurídica a la que el ordenante solicita que le sea entregado un documento electrónico.
- **Tercero de confianza:** 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.

2.4. Modelo lógico ERDS

El modelo lógico ERDS aplicado es el de caja negra (Black-box model), con ANF AC como único ERDSP.

2.5. Estilo de operación

2.5.1. Almacenamiento y Reenvío (S&F)

Se permite el envío de contenido directamente a la plataforma del destinatario sin requerir una acción del destinatario.

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

- utilizan el protocolo de transferencia SMTP (correo electrónico),
- ofrecen la opción a todos los usuarios de enviar y recibir mensajes en formato MIME según RFC 2045 e RFC 5322

No soporta interconexión con otros REMS.

2.5.2. Almacenamiento y Notificación (S&N)

Tanto QERDS como ERDS permiten el estilo S&N, en el que se envía al destinatario una referencia al contenido de usuario y se requiere que el destinatario responda activamente en la plataforma si acepta o rechaza el mensaje entrante, antes de la consignación. Solo se produce la consignación del contenido del usuario si la respuesta fue positiva.

El servicio no permite el estilo S&N para mensajes transmitidos por otro ERDS (REMS).

Sign to sign ofrece al ordenante la posibilidad de establecer un periodo de validez y fecha de caducidad determinados para aceptación o rechazo de las comunicaciones enviadas siguiendo el estilo S&N, y se informa al destinatario de dicho plazo.

2.6. 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.

2.6.1. Identificación inicial del ordenante

La identidad del ordenante se verificará antes del inicio del servicio por el Responsable de Verificación de Identidad mediante 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.

El nivel de seguridad de esta identificación para el servicio QERDS es de Nivel Alto.

El nivel de seguridad de esta identificación para el servicio ERDS es de Nivel medio/sustancial.

Esta identidad verificada se vinculará al usuario de dicho ordenante, y a un medio de autenticación.

2.6.2. Identificación del destinatario

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

En el servicio QERDS, la identidad del destinatario se verificará antes de cada entrega mediante 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 destinatario se verificará por uno de los medios de identificación de nivel de seguridad bajo (Art. 8.2.a) del Reglamento eIDAS).

ANF AC puede vincular la identidad ya verificada anteriormente del destinatario a un medio de autenticación indicado en el requerimiento REQ-QERDS-5.2.2-03 de la ETSI EN 319 521.

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.

2.6.3. 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.

2.7. Ámbito de aplicación

2.7.1. 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.

2.7.2. 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 Declaración de Prácticas 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.

2.8. Términos y condiciones del servicio

Ver el documento de Términos y condiciones publicado en https://www.anf.es/ac-repositorio-legal-terminos-y-condiciones/

3. Eventos, evidencias y documento probatorio

Todas las prácticas definidas 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.

3.1. Evidencias almacenadas por el servicio

3.1.1. Evidencias de identidad

La información registrada es, como mínimo:

- Prueba de la verificación inicial de la identidad del ordenante;
- Datos de identificación de los ordenantes;
- Datos de autenticación de los ordenantes;
- Registros de la operación del ERDS, verificación de identidad del ordenante y destinatario y comunicación;
- Prueba de la verificación de la identidad del destinatario antes del envío / entrega del contenido del usuario;

3.1.2. Evidencias del contenido de usuario

- Medios para demostrar que el contenido del usuario no ha sido modificado durante la transmisión y almacenamiento. Los documentos electrónicos del contenido de usuario se sellan electrónicamente, lo que permite comprobar que no han sido modificados entre el envío y la recepción.
- Referencia o un resumen del contenido completo del usuario enviado;
- Tokens de sello de tiempo correspondientes a la fecha y hora de envío, consignación y entrega del contenido del usuario.

3.1.3. Evidencias sobre la trazabilidad de la orden de entrega

Tokens de sello de tiempo correspondientes a la fecha y hora de envío, consignación y entrega del contenido del usuario.

Eventos relativos al envío	
Aceptación de la orden de entrega certificada *(Submission Acceptance)*	El ordenante, debidamente autenticado en el servicio, ha transmitido al ERDS (ANF AC – Sign to sign), en el momento indicado en la evidencia, una solicitud de comunicación con un contenido de usuario y una especificación de los requerimientos de entrega. ANF AC, ha verificado la solicitud y ha aceptado el encargo de entrega certificada al destinatario y al buzón indicado.
Denegación de la prestación del servicio	La entrega electrónica certificada solicitada por el ordenante, no fue aceptada por el ERDS (ANF AC – Sign to sign). El prestador del servicio puede rechazar una solicitud siempre que lo considere oportuno, ya sea por razones de políticas, comerciales, formales o técnicas. El ERDS, previo a la transmisión del documento electrónico,

(Submission Rejection)	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 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.
Eventos relativos a la notificación de entrega por parte del destinatario	
Notificación para la aceptación *(Notification For Acceptance)*	El ERDS (ANF AC – Sign to Sign) notifica al destinatario que tiene una comunicación/entrega disponible (sin divulgar necesariamente el ordenante, contenido, etc.) y le permite acceder a la plataforma de entrega para aceptarlo, rechazarlo o ignorarlo. Esta notificación también podrá indicar que se solicitará una acción explícita que acredite la conformidad del destinatario al contenido del documento electrónico entregado. La evidencia relacionada atestigua que el destinatario recibió y abrió la notificación en el buzón indicado, en un momento específico según lo indicado por la evidencia. La evidencia no atestigua que esa notificación fuera leída por el destinatario.
Fallo en la notificación para la aceptación *(Notification For Acceptance Failure)*	No se pudo entregar la notificación 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. La evidencia relacionada atestigua que una notificación de entrega disponible no se pudo enviar al destinatario especificado después de un cierto número de intentos o un tiempo de espera determinado.
Eventos relativos a la consignación al destinatario	
Aceptación de la consignación *(Consignment Acceptance)*	El destinatario realizó una acción explícita (p.ej. 2FA) indicando al ERDS la aceptación de recibir el contenido de usuario. La evidencia atestigua que el destinatario, tras 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.
Consignación del contenido *(Content Consignment)*	ANF AC – Sign to sign, confirma que el contenido de usuario se ha puesto a disposición del destinatario dentro de los límites de la aplicación. La evidencia relacionada atestigua que, el contenido de usuario, en un momento específico indicado por la evidencia, se puso a disposición del destinatario.
Rechazo de la consignación *(Consignment Rejection)*	El destinatario, tras una identificación y autenticación adecuadas, realizó una acción explícita que indica que rechaza recibir el contenido 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.
Fallo técnico en la consignación del contenido *(Content Consignment Failure)*	El contenido del usuario no se pudo poner a disposición del 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. Este evento puede ser desencadenado por diferentes motivos, por ejemplo: • El sistema no pudo consignar el contenido del usuario al destinatario. • El sistema 2FA no pudo transmitir con éxito el código de verificación o QR al destinatario. • Documento cifrado corrupto • Fallo de integridad del documento electrónico • Detección de contenido ilícito La evidencia relacionada atestigua que el contenido no pudo estar disponible para el destinatario dentro de un período de tiempo dado fallo técnico de la aplicación del ERDS.
Caducidad de la aceptación / rechazo *(Acceptance Rejection Expiry)*	ANF AC – Sign to sign envió una notificación al destinatario, pero no respondió a dicha notificación con una aceptación/rechazo pasado un plazo de tiempo determinado. Este período de tiempo puede determinarse mediante legislación, reglas de política del ERDS, o parámetros dados por el ordenante. Por defecto, se establecerá un periodo de caducidad de 2 meses. La evidencia relacionada atestigua que la notificación orden de entrega caducó en el momento indicado por la evidencia, tras la falta de respuesta del destinatario.
Eventos relativos a la descarga del contenido por el destinatario	
Entrega del contenido *(Content Handover)*	El documento electrónico fue entregado y descargado por el destinatario. La evidencia relacionada atestigua que el documento electrónico consignado por el ordenante, en un momento específico fue transmitido íntegramente al destinatario.
Fallo de entrega del contenido *(Content Handover Failure)*	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.
Otros eventos específicos del ERDS ANF AC Sign to sign	
Adhesión a un documento electrónico	El destinatario realizó una acción explícita (p.ej. firma electrónica, firma grafométrica, 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 a ANF AC para que, en calidad de mandatario, firme en su nombre la conformidad de aceptación del contenido del documento electrónico.
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.
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.

3.2. Documento probatorio

Las evidencias del conjunto de eventos producidos en cada orden de entrega electrónica certificada del servicio se recopilan en un único documento PDF denominado "Documento Probatorio". Este documento está identificado con un código único y autenticado mediante sello electrónico cualificado de ANF AC[2], incluyendo comprobación OCSP y sello cualificado de tiempo electrónico.

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.

Consta de un acta general que contiene información sobre el contenido electrónico recibido y transmitido, identidad del ordenante y del destinatario, así como todos los eventos que se han generado durante el proceso de envío (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 ocurrieron y el resultado obtenido. De cada evento concreto también se incluye un acta específica con la información detallada.

El documento probatorio establece la modalidad de servicio prestado según cualificación.

Para la obtención de documentos probatorios, se proporcionan los siguientes métodos:

- Mediante la ERD-UA: 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.
- Personación en las oficinas administrativas (sección 1.4.) de ANF AC: 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.

[2] *PAdES-BASELINE-LT conforme ETSI EN 319 142-1 y 319 142-2*

Solo accesibles a:

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

3.3. Logs del servicio

ANF AC mantiene un registro de los logs relacionados con:

- Todos los eventos identificados en el punto 3.1.
- Cambios relacionados con la política de seguridad.
- Puesta en marcha y apagado del sistema.
- Caídas del sistema y fallos de hardware.
- Actividades de firewall y router.
- Intentos de acceso al sistema PKI.

Cada evidencia está autenticada mediante sello electrónico de ANF AC que incluye comprobación OCSP y sello cualificado de tiempo electrónico.

3.3.1. Frecuencia de procesado

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

3.3.2. 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 2 años y durante un periodo de hasta 15 años en backup.

3.3.3. Limitaciones al periodo de validez

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

4. Obligaciones y responsabilidades

4.1. Obligaciones del ERDSP (ANF AC)

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 tal y como se especifica en su DPC. Se obliga a:

- Respetar lo dispuesto en esta declaración de prácticas.
- Responder por el incumplimiento de lo establecido en esta declaración de prácticas y, allí donde sea aplicable.
- Publicar y mantener actualizada esta declaración de prácticas.
- Informar sobre las modificaciones de esta declaración de prácticas a clientes y terceros que confían en los servicios.
- Utilizar certificado de sello electrónico que identifica el servicio de entrega electrónica certificada y destinarlo a ese único fin.
- 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.
- Proceder a la validación de las firmas y sellos electrónicos mediante un servicio cualificado de validación en conformidad con la normativa vigente.
- 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.
- 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.
- 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.

4.1.1. Responsabilidad financiera

Se aplica lo establecido en la DPC de ANF AC. En cuanto a 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 €)

4.1.2. Exoneración de responsabilidad

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. NF AC no se hace responsable en caso de pérdidas por transacciones.

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 la presente Declaración de Prácticas 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 contenido de los mensajes o documentos utilizados.
- En relación a acciones u omisiones del Cliente.
- Falta de veracidad de la información suministrada como contenido de usuario para la prestación del servicio.
- Negligencia del usuario 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 Declaración de Prácticas 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.
- La intervención de ANF AC no puede presuponer adhesión al contenido del mensaje, ni ANF AC es responsable del mismo. ANF AC no revisa el contenido de las comunicaciones, no obstante lo anterior, si llegara a advertir por cualquier medio que el contenido que se quiere transmitir es ilícito, procederá a denegar el servicio ANF AC no revisa los contenidos de las comunicaciones del ordenante, interviene como mero proveedor del servicio de comunicaciones.
- 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.

4.2. Obligaciones del ordenante y destinatario

- Respetar lo dispuesto en esta declaración de prácticas.
- Proteger sus credenciales de acceso y certificado electrónico cualificado 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.
- No aplicar ingeniería inversa y la búsqueda de fallos en la lógica del sistema, lo cual está prohibido.
- 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.

4.3. 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 esta declaración de prácticas.
- Reportar cualquier incidente de seguridad tan pronto como este sea identificado.
- Tener en consideración otras precauciones descritas en acuerdos u otros sitios.

4.4. Obligaciones de las organizaciones externas

ANF AC se asegura que el proveedor de servicios de almacenamiento (AWS) disponga de las medidas establecidas para garantizar confidencialidad y disponibilidad de la información.

4.5. Resolución de conflictos

- **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.
- **Jurisdicción competente:**
  La relación entre ANF AC y las partes que confían se rige exclusivamente por la legislación española.

5. Gestión y operación del QERDSP

5.1. Controles de seguridad física y ambiental

Según lo definido en la DPC de ANF AC.

5.2. Controles operativos

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.

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/TLS entre los usuarios y los sistemas del ERDS, y entre sistemas informáticos. Los gestores de bases de datos se encuentran en la misma red interna que el resto de los subsistemas del ERDS, con lo cual no requieren de conexión segura, pues no son accesibles fuera de dicha red.

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 lógica establecidas en la DPC y adenda de ANF AC. ANF AC garantiza la confidencialidad, integridad y disponibilidad de los registros.

5.3. Controles criptográficos

Las claves de firma se encuentran físicamente aisladas de las operaciones normales, de tal manera que solo el personal de confianza designado tiene acceso a las claves para su uso en el sellado electrónico del contenido y/ o documento probatorio.

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.

5.4. 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 declaración de prácticas 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.
- **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.

5.5. Gestión de incidentes

ANF AC dispone de un Registro de Incidentes en el que se inscribe toda incidencia que se haya producido con los servicios, 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.

5.6. Seguridad de red

Según lo definido en la DPC de ANF AC.

5.7. 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.

6. Cese del servicio QERDS

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

6.1. 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.

6.1.1. 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 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.

6.1.2. 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.

6.1.3. Transferencias 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.

6.1.4. 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.

6.1.5. Transferencias de la gestión del servicio

No se contempla la transferencia de la gestión del servicio.

6.2. 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.