Servicio de Firma Electrónica Cualificada Remota (SPPS) de ANF AC

Declaración de Prácticas y Política del Servicio

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

Teléfono: 932 661 614

www.anf.es

Nivel de Seguridad

Documento Público

Aviso Importante

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

Teléfono: 932 661 614

www.anf.es

INDEX

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.

La Infraestructura de Clave Pública (PKI) de ANF AC sigue las directrices del Reglamento [UE] 910/2014, de 23 de julio de 2014, del Parlamento Europeo y del Consejo (en adelante "eIDAS"), y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

1.1. Objetivo y alcance

El presente documento recoge la Política y Prácticas del Servicio de Firma Electrónica Cualificada Remota (SPPS) prestado por ANF AC. Este documento forma parte integrante de la Declaración de Prácticas de Certificación (DPC) de ANF AC, como Prestador Cualificado de Servicios de Confianza (PCSC).

El sistema de gestión centralizada de certificados y servicio de firma remota de ANF AC consiste en la gestión, en nombre del firmante, de su dispositivo de creación de firma. De este modo, los suscriptores pueden emplear certificados cualificados cuyas claves privadas se alojan y administran de manera segura en un dispositivo **QSCD** (bajo el modelo *managed on behalf*). Así se facilita la generación de firmas electrónicas cualificadas de forma remota, garantizando que el firmante conserve en todo momento el control exclusivo sobre sus claves de firma.

Este documento describe los aspectos más relevantes del **Servicio de firma remota**, así como la operativa de los componentes que gestionan los dispositivos de creación de firma a distancia en nombre del firmante. Asimismo, incluye una declaración de las medidas de salvaguarda de la infraestructura y de los controles de seguridad técnicos y no técnicos aplicados a los sistemas que participan en la prestación del servicio.

La presente **Política y Declaración de Prácticas** se aplica a las claves de todos los certificados cualificados de firma electrónica definidos en la DPC de ANF AC como

en soporte "centralizado" o certificado centralizado.

Este documento se ha estructurado tomando como referencia la especificación técnica **ETSI TS 119 431**.

1.2. Resumen del servicio

El sistema de generación de firmas electrónicas cualificados remotas de ANF AC está formado por los siguientes elementos:

1. **HSMs nShield Connect XC**
2. **Software *Signature Activation Module* (SAM) de Entrust,** que garantiza que el usuario mantenga el control exclusivo de sus claves de firma
3. **Servidores DELL (tamper proof),** que protegen la infraestructura física de la solución
4. **Software de firma** desarrollado por ANF AC

Estos componentes se integran para proporcionar un servicio de firma electrónica cualificada remota fiable y seguro. Los HSMs nShield Connect XC custodian las claves de forma segura; el SAM de Entrust asegura que únicamente el titular de la clave puede activarla y utilizarla; los servidores DELL con capacidad "tamper proof" refuerzan la integridad física de la plataforma; y el software de firma de ANF AC coordina la generación de firmas electrónicas cualificadas de manera remota.

1.3. Nombre del documento e identificación

Nombre del documento	Declaración de Prácticas y Política del Servicio de Firma Electrónica Cualificada Remota (SPPS)		
Versión	1.2		
OID	1.3.6.1.4.1.18332.3.4.1 0.4.0.19431.1.1.3 - EUSCP: EU SSASC Policy		
Fecha de aprobación	10/02/2026	**Fecha de publicación**	10/02/2026
DPC relacionada	Declaración de Prácticas de Certificación (DPC) de ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1		

1.3.1. Administración de la Política

Según lo establecido en la DPC de ANF AC.

1.3.2. Revisiones

Versión	Cambios	Aprobación	Publicación
1.2.	Revisión anual.	10/02/2026	10/02/2026
1.1.	Revisión anual.	23/12/2024	23/12/2024
1.0.	Creación del documento	19/02/2023	19/02/2023

1.4. Entidades Participantes

En la provisión y utilización de los Servicios de Confianza regulados en la presente DPC, intervienen las siguientes partes:

1. ANF AC - Proveedor del servicio de firma remota (SSASP)
2. Autoridad de Registro (RA)
3. Suscriptores y firmantes de los certificados
4. Terceros que confían en los certificados

1.4.1. Autoridades de Certificación (CA) – Proveedor del servicio de firma remota (SSASP)

El *componente de servicio de aplicación de firma en remoto (SSASC)* forma parte de los servicios operados por ANF AC y permite prestar el servicio de firma electrónica a distancia a aquellos firmantes que dispongan de un certificado cualificado de firma electrónica **centralizado** conforme a lo establecido en la DPC de ANF AC.

ANF AC actúa como proveedor del servicio de aplicación de firma en servidor (SSASP) y no delega ninguna parte de dicha prestación en entidades externas. En su calidad de SSASP, ANF AC desarrolla, implementa, hace cumplir y actualiza este documento, que contiene la Política y la Declaración de Prácticas de SPPS.

1.4.2. Autoridad de Registro (RA)

Según lo establecido en la DPC de ANF AC.

1.4.3. Suscriptor y firmante

El Suscriptor es la persona física o jurídica que ha contratado los servicios de confianza de ANF AC y que, por lo tanto, será el propietario del certificado. En consecuencia, tendrá los derechos de revocación y suspensión sobre el certificado.

Los Firmantes son las personas físicas que mantienen bajo su uso exclusivo los datos de creación de firma asociados a los Certificados de los que son Titulares. El Firmante es quien crea la firma electrónica, para lo cual debe estar identificado por su nombre, apellidos y NIF, NIE o número de pasaporte.

El Suscriptor de un Certificado puede diferenciarse de la figura del Firmante cuando existe una relación de representación o pertenencia a una Organización, de modo que esta última actúe como la entidad Suscriptora, o en el caso de Certificados de Sello electrónico. No obstante, cada Declaración de Políticas de Certificación Particulares determinará la posible separación entre las figuras de Firmante y Suscriptor.

1.4.4. Terceros que confían en los certificados

Las partes que confían son aquellas personas físicas o jurídicas distintas del Firmante o Suscriptor que reciben y/o emplean los certificados o las firmas electrónicas emitidos por ANF AC.

Los certificados centralizados cubiertos en esta Política cumplen con los requisitos que establece la Ley 6/2020 y el Reglamento eIDAS, y están reconocidos por @firma, la plataforma de validación y firma electrónica del Gobierno de España.

Los terceros que confíen en estos certificados deberán tener en cuenta las limitaciones de uso, tanto cuantitativas como cualitativas, especificadas en la DPC, en este documento y en el propio certificado.

1.5. Uso de los certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de ANF AC y en la Política de Certificación (PC) correspondiente de cada certificado.

1.6. Definiciones y acrónimos

1.6.1. Definiciones

A las definiciones dispuestas en la DPC de ANF AC, para la interpretación del presente documento se añaden los siguientes términos tal y como se definen en ETSI TS 119 431-1:

identificación electrónica (eID): el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.

medios de identificación electrónica: una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.

referencia a medios de identificación electrónica: datos usados en el SSASC como referencia a unos medios de identificación electrónica que permiten autenticar a un firmante.

dispositivo cualificado de creación de firma / sello electrónico (QSCD): dispositivo de creación de firma que cumple con los requisitos del Anexos II del Reglamento(EU) No 910/2014.

dispositivo remoto de creación de firma: dispositivo de creación de firma utilizado a distancia por el firmante y operado en su nombre bajo su control exclusivo de uso.

componente de servicio de aplicación de firma en servidor (SSASC): componente de servicio operado por un TSP, compuesto de una aplicación de firma en servidor (SSA) y un QSCD / SCdev, empleado para la creación de firmas electrónicas en nombre del firmante.

proveedor de servicio de aplicación de firma en servidor (SSASP): TSP que opera un SSASC.

dispositivo de creación de firma (SCDev o SCD): un equipo o programa informático configurado que se utiliza para crear una firma electrónica.

1.6.2. Acrónimos

EUSPv2: Política SSAS de la UE v2

QSCD: Dispositivo Cualificado de Creación de Firma/Sello Electrónico

SAD: Datos de Activación de Firma

SAM: Módulo de Activación de Firma

SAP: Protocolo de Activación de Firma

SCDev: Dispositivo de Creación de Firma

SP: Política SSAS

SSAS: Servicio de Aplicación de Firma de Servidor

SSASP: Proveedor de Servicios de Aplicación de Firma de Servido

TW4S: Trustworthy System Supporting Server Signing

2. Repositorios y publicación de información

2.1. Repositorios

Según lo establecido en la DPC de ANF AC.

2.2. Publicación de información de certificación

Según lo establecido en la DPC de ANF AC.

2.3. Momento y frecuencia de publicación

Según lo establecido en la DPC de ANF AC.

2.4. Controles de acceso a los repositorios

Según lo establecido en la DPC de ANF AC.

3. Identificación y autenticación

3.1. Registro de Nombres

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de ANF AC y en la Política de Certificación (PC) correspondiente de cada certificado.

3.2. Validación inicial de la identidad

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de ANF AC y en la Política de Certificación (PC) correspondiente de cada certificado.

3.3. Identificación y autenticación para solicitudes de renovación de claves

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de ANF AC y en la Política de Certificación (PC) correspondiente de cada certificado.

3.4. Identificación y autenticación para solicitud de revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de ANF AC y en la Política de Certificación (PC) correspondiente de cada certificado.

4. Requisitos operacionales del ciclo de vida de las claves de firma

La solicitud, tramitación de dichas solicitudes, aceptación, renovación, modificación, y revocación del certificado centralizado se rigen por lo dispuesto en la Declaración de Prácticas de Certificación (DPC) y en la Política de Certificación (PC) aplicable a cada tipo de certificado. En este documento únicamente se describen los aspectos específicos que afectan al servicio de firma remota y a los certificados centralizados, completando lo ya establecido en la DPC y la PC correspondientes.

4.1. Inicialización de las claves de firma

ANF Autoridad de Certificación, en la prestación de su servicio de firma en servidor, emplea dispositivos criptográficos de creación y protección de firmas clasificados como cualificados (QSCD), en cumplimiento con el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre la identificación electrónica y los servicios de confianza en el mercado interior (Reglamento eIDAS), que deroga la Directiva 1999/93/CE.

Los HSM utilizados se encuentran certificados bajo Common Criteria EAL4+ (AVA_VAN.5 y ALC_FLR.2), y la solución SSASC empleada se alinea con los requisitos de seguridad establecidos en la norma EN 419 241-1, lo que permite operar como un Trustworthy System Supporting Server Signing (TW4S) con Sole Control Level 2 (SCAL2).

ANF AC garantiza que la operación de QSCD empleado, cumplen en todo momento con los requisitos, condiciones y restricciones establecidos en el informe de certificación correspondiente a dicho dispositivo. En particular:

- Los requisitos técnicos, operativos y de configuración definidos en el informe de certificación del QSCD remoto son aplicados y mantenidos durante toda la fase de explotación del servicio.
- Cualquier limitación de uso, hipótesis operativa, requisito organizativo o medida de seguridad indicada en el informe de certificación es incorporada a los procedimientos, controles y medidas de seguridad del SSASP.
- ANF AC no opera el remote QSCD fuera de las condiciones evaluadas y certificadas, ni introduce cambios que puedan afectar al estado de certificación sin realizar previamente la evaluación y gestión de riesgos correspondiente.
- Las actualizaciones, cambios de configuración o modificaciones operativas del SSASP y del QSCD remote se gestionan de forma controlada, garantizando la continuidad del cumplimiento con los requisitos del informe de certificación.

4.1.1. Generación de las claves de firma

El Servicio de Aplicación de Firma en Servidor (SSASC) de ANF AC utiliza un software de firma propio, en combinación con el Software Signature Activation Module (SAM) de Entrust, instalado en servidores tamper proof, junto con un módulo criptográfico (HSM) nShield Connect XC clasificado como QSCD. Dicho HSM ha sido validado para cumplir, al menos, con los requisitos de FIPS 140-2 nivel 3 o FIPS 140-3 nivel 3, permitiendo realizar todas las operaciones criptográficas con las claves de los firmantes y garantizando el control exclusivo por parte de cada titular. El SAM de Entrust cumple con la norma CEN EN 419 241-2 y actualmente está certificado según la certificación Common Criteria asociada.

Las operaciones de inicialización y administración del módulo criptográfico requieren control dual. Una vez finalizado el proceso de registro, se generan las claves RSA de 3072 bits del usuario dentro del HSM. Hasta que se produzca la emisión del certificado por parte de ANF AC, dichas claves permanecen en estado no activo, sin posibilidad de uso.

Junto a la clave del firmante, se genera una petición de certificado en formato PKCS#10 que actúa como prueba de posesión de la clave privada durante el proceso de registro y emisión del certificado ante la Autoridad de Certificación. Cuando el certificado ha sido emitido y validado, las claves se activan, habilitando la generación de firmas electrónicas cualificadas.

En caso de requerirse copias de seguridad, las claves se almacenan cifradas fuera del HSM mediante el algoritmo AES con longitud de 128 bits, derivado de una clave maestra interna del HSM, garantizando la confidencialidad e integridad de las claves en todo su ciclo de vida.

4.1.2. Asociación de los medios de identificación electrónica del firmante

Tras tramitarse la solicitud a través de un operador autorizado de una Oficina de Verificación Presencial (OVP) en AR Manager, el solicitante recibe un correo electrónico con un enlace único que le permite acceder a la pasarela web de confirmación de la solicitud (https://activatucertificado.anf.es/).

En dicha pasarela, el solicitante debe introducir dos códigos de confirmación previamente facilitados: uno por SMS y otro a través del correo electrónico. A continuación, puede revisar los datos de la solicitud y debe establecer sus credenciales con doble factor de autenticación, así como un PIN, que actuará como dato de activación del certificado.

Una vez el solicitante confirma la solicitud, el sistema pide al Servicio de Aplicación de Firma en Servidor (SSASC) la generación del par de claves de firma y registra la solicitud, que se remite a los servidores de ANF AC para la revisión por parte de los Responsables de Dictámenes de Emisión. Acto seguido, ANF AC procede a la emisión del certificado electrónico y solicita al SSASC su vinculación con el par de claves generado.

El uso de la clave privada queda condicionado a la activación de los dos factores de autenticación de distinta categoría. Asimismo, el SSASC protege la integridad de las claves y los metadatos asociados, gestionándolos en una base de datos cifrada.

4.1.3. Asociación del certificado del firmante

Una vez completados los procesos de registro y emisión del certificado del firmante, dicho certificado se importa en el Servicio de Aplicación de Firma en Servidor (SSASC). El SSASC verifica que la clave pública incluida en el certificado coincide con la almacenada en el sistema. En caso de correspondencia, el certificado queda vinculado al par de claves del firmante, conformando así su identidad de firma (identificador único; compuesto por el certificado y la clave privada generada en el dispositivo QSCD).

Hasta que el certificado no se asocia efectivamente con su correspondiente par de claves, la identidad de firma permanece incompleta, y el SSASC no permite usar las claves para firmar. Una vez se vinculan ambas partes, la clave del firmante pasa a estar operativa para realizar operaciones de firma, siempre que se hayan activado los factores de autenticación requeridos.

El SSASC protege la integridad de las claves de los firmantes y sus metadatos asociados mediante su almacenamiento seguro y asegura la validez de cada identidad de firma mediante procedimientos de registro que conservan trazabilidad e integridad de la información.

4.1.4. Provisión de los medios de identificación del firmante

Cuando el firmante confirma su solicitud a través de la pasarela web segura de ANF Autoridad de Certificación (ANF AC), se habilita un proceso para configurar sus medios de identificación electrónicos, incluidos credenciales y un doble factor de autenticación. En ese momento, se genera y asocia al firmante un código o semilla necesaria para la emisión de contraseñas de un solo uso (OTP), sin que dicha información se almacene en texto claro.

El Servicio de Aplicación de Firma en Servidor (SSASC) únicamente conserva la información imprescindible para validar los OTP generados por el firmante, garantizando la confidencialidad de sus datos de acceso y evitando exponer las claves o contraseñas en formato legible.

4.2. Uso de las claves y el certificado

4.2.1. Activación de las claves de firma

Para cada uso de la clave de firma, el firmante debe enviar un mensaje de activación de firma (SAD) a través del protocolo de activación de firma (SAP). Este mensaje incluye dos factores de autenticación de distinta categoría y un testigo de sesión. Previamente, el firmante se identifica con su usuario y al menos un factor de autenticación para obtener dicho testigo de sesión.

Las claves del firmante únicamente pueden activarse si el HSM se encuentra operativo.

El SSASC valida que el SAD sea correcto, y solo cuando el firmante se ha autenticado de forma adecuada (mediante credenciales y factores de autenticación) la clave queda activa. Una vez activada, el SSASC permite un único uso para firmar el resumen criptográfico contenido en el SAD; al completarse la operación, la clave se desactiva, requiriéndose un nuevo SAD para cada firma posterior.

El protocolo SAP está diseñado para prevenir ataques de tipo *man-in-the-middle* y *replay*. El mensaje SAD incorpora salvaguardas contra suplantación, robo de sesión, duplicación, robo de credenciales, phishing y adivinación, mediante técnicas de cifrado, firma electrónica, funciones resumen, números aleatorios y el uso de dos factores de autenticación de distinta naturaleza (algo que el firmante conoce y algo que el firmante posee).

Si el firmante introduce su factor de activación de forma incorrecta en tres ocasiones consecutivas, el acceso a la clave remota queda bloqueado. El desbloqueo solo puede realizarse mediante un proceso de recuperación que se envía al correo electrónico del titular.

Todas las comunicaciones con el SSASC se protegen mediante TLS 1.2.

Los controles de acceso del SSASC garantizan que un firmante no pueda acceder a las claves de otros usuarios ni a funcionalidades del sistema distintas de las necesarias para la firma o su gestión personal.

Las claves de firma solo están activas (sesión de firma) en el momento de realizar cada firma puntualmente. Una vez realizada la firma, se desactivan nuevamente. De esta forma, no existe una sesión de firma activa durante un periodo de tiempo superior a 30 minutos; la sesión de firma tiene un tiempo de vida de unos segundos para realizar la firma.

Asimismo, el SSASC conserva la fecha de caducidad y el estado de revocación del certificado asociado a la clave; si el certificado ha caducado o está revocado, se deniega el uso de la clave.

Por último, las claves de los firmantes se almacenan cifradas empleando AES (256 bits), derivado de una clave maestra del módulo criptográfico. El módulo SAM, junto con el HSM, permite generar firmas electrónicas bajo el estándar RSA PKCS#1 v1.5 con funciones resumen SHA-256, SHA-384 o SHA-512, según corresponda, garantizando la integridad y la autenticidad de los datos firmados.

4.2.2. Borrado de las claves de firma

Las claves del firmante se eliminan de forma inmediata cuando su certificado es revocado.

De manera periódica, ANF AC ejecuta un proceso que suprime las claves de aquellos firmantes cuyo certificado asociado ha caducado.

Los firmantes pueden solicitar la revocación de su certificado siguiendo los procedimientos establecidos en la DPC de ANF AC. En todos los casos, la revocación o la caducidad del certificado conlleva la destrucción de las claves asociadas.

4.2.2.1. Copia de seguridad y restauración de las claves de firma

Las claves de los firmantes están protegidas por la clave maestra del módulo criptográfico y únicamente pueden utilizarse cuando este se encuentra activo. Durante la realización de copias de seguridad de las claves de los firmantes, se emplea el algoritmo de cifrado AES con una longitud de clave de 128 bits. Periódicamente, se generan copias de seguridad de la

base de datos del SSA, donde se encuentran referenciadas las claves de los firmantes, así como del resto de claves de infraestructura necesarias para garantizar la continuidad del servicio en caso de incidente, manteniéndose el número de copias al mínimo imprescindible.

Las claves de infraestructura del SSASC se almacenan en contenedores cifrados. El módulo criptográfico que contiene la clave maestra del SSASC, encargada de proteger las claves de todos los firmantes, requiere de control dual para su operación, copia de seguridad y restauración. Esta clave maestra nunca abandona el módulo criptográfico en texto claro.

5. Controles de seguridad física, de gestión y de operaciones

5.1. Controles de seguridad física

Según lo establecido en la DPC de ANF AC.

5.2. Controles de procedimientos

Según lo establecido en la DPC de ANF AC.

5.3. Controles de personal

El SSA implementa los siguientes roles de gestión:

- **Responsable de seguridad (security officer):** tiene la responsabilidad general de administrar e implementar las políticas de seguridad y tiene acceso a la información de seguridad.
- **Administrador del sistema (system administrators):** es el responsable de instalar, configurar y mantener el TW4S pero con acceso controlado a la información de seguridad.
- **Operador del sistema (system operators):** es el responsable de la operación del día a día del TW4S y las operaciones de copia de seguridad y restauración.
- **Auditor del sistema (system auditor):** está autorizado para revisar los archivos y registros de auditoría del TW4S para auditar que las operaciones del sistema están alineadas con la política de seguridad.

ANF AC asigna estos roles a personal cualificado e implementa todos los controles de segregación de funciones definidos en la sección 6.2.1.2 de la norma CEN EN 419 241-1.

5.4. Procedimientos de auditoría de seguridad

Según lo establecido en la DPC de ANF AC. Además, en particular, en la prestación del servicio de firma electrónica en remoto:

El Servicio de Aplicación de Firma en Servidor (SSASC) registra, al menos, los siguientes eventos:

- Inicialización, arranque, parada y cambios de configuración del sistema.
- Eventos de gestión de claves del firmante (generación, activación, uso, desactivación y destrucción).
- Uso de claves de los firmantes.
- Autenticaciones de los firmantes (incluyendo los intentos fallidos).
- Cambios relacionados con los datos de activación de firma (por ejemplo, cambios de PIN).
- Arranque, parada y reconfiguración de las funciones de auditoría.
- Accesos al sistema por parte de los usuarios administradores.

El SSASC genera un registro de auditoría continuo en el que únicamente es posible añadir nuevos eventos, sin posibilidad de eliminar ni modificar los ya existentes. Para proteger cada entrada del registro y el registro en su totalidad, se aplican técnicas que encadenan cada evento con el anterior, impidiendo la manipulación de los datos registrados. Periódicamente y durante el arranque, el SSASC verifica la integridad de dicho registro, contando además con una funcionalidad que permite a un usuario con rol de auditor efectuar la misma comprobación bajo demanda.

A fin de garantizar la exactitud de la fecha y hora de los eventos de auditoría, el reloj de los sistemas se sincroniza mediante NTP, tomando como referencia el Real Observatorio de la Armada (ROA), y se implementan controles que permiten detectar incidencias que pudieran afectar dicha sincronización.

En caso de que las funciones de auditoría dejen de estar disponibles, el SSASC suspenderá automáticamente el procesamiento de nuevas peticiones, asegurando que no se realice ninguna operación sin el debido control.

5.5. Archivo de informaciones

Según lo establecido en la DPC de ANF AC.

5.6. Cambio de claves

Según lo establecido en la DPC de ANF AC.

5.7. Compromiso de claves y recuperación de desastre

Según lo establecido en la DPC de ANF AC.

5.8. Cese de actividad

Según lo establecido en la DPC de ANF AC.

6. Controles de seguridad técnica

Según lo establecido en la DPC de ANF AC, excepto las siguientes cuestiones específicas del servicio de firma remota cualificada:

6.1. Operaciones y sistemas

La entidad dispone de procedimientos para operar de forma correcta y segura el SSASC.

El componente software SSA, el Entrust SAM y el módulo HSM son operados de acuerdo con sus manuales para su instalación, administración y operación para cumplir con los objetivos de seguridad definidos en la Declaración de Seguridad de su certificación como dispositivo QSCD.

6.2. Controles de seguridad informática

Según lo establecido en la DPC de ANF AC.

El SSASC se encuentra monitorizado y se generan alertas que son enviadas a los administradores del sistema cuando se detectan eventos que pueden impactar en su disponibilidad o comprometer su seguridad.

7. Perfiles de los certificados, CRL y OCSP

7.1. Perfil del certificado

7.1.1. Número(s) de versión

Según lo establecido en la DPC de ANF AC.

7.1.2. Extensiones del certificado

Las extensiones utilizadas por cada tipo de certificado emitidos bajo la presente política se publican en el documento denominado "Perfiles de los certificados de ANF AC" en la web de ANF AC (https://anf.es/repositorio-legal/)

7.1.3. Identificadores de objetos de algoritmos

Según lo establecido en la DPC de ANF AC.

7.1.4. Formas del nombre

Según lo establecido en la DPC de ANF AC.

7.1.5. Restricciones del nombre

Según lo establecido en la DPC de ANF AC.

7.1.6. Identificador del objeto de la política del certificado

Bajo las disposiciones establecidas en este documento, se emiten los siguientes tipos de certificados, junto con sus OID correspondientes:

Tipo	Soporte		OID
Clase 2 de Persona Física	QSCD. Servicio Centralizado		1.3.6.1.4.1.18332.3.4.1.5.22
Corporativo de Colegiado	QSCD. Servicio Centralizado		1.3.6.1.4.1.18332.3.4.1.11.22
Representante Legal de Persona Jurídica	QSCD. Servicio Centralizado		1.3.6.1.4.1.18332.2.5.1.14
Representante Legal de Entidad sin Personalidad Jurídica	QSCD. Servicio Centralizado		1.3.6.1.4.1.18332.2.5.1.15
Representante Legal para administradores únicos y solidarios	QSCD. Servicio Centralizado		1.3.6.1.4.1.18332.2.5.1.13
Sello Electrónico *(QSealC)*	QSCD. Servicio Centralizado		1.3.6.1.4.1.18332.25.1.1.9
Sello Electrónico AA.PP. *(QSealC AA.PP.)*	Nivel Alto	QSCD. Servicio Centralizado	1.3.6.1.4.1.18332.25.1.1.11
Sello Electrónico PSD2 *(QSealC PSD2)*	QSCD. Servicio Centralizado		1.3.6.1.4.1.18332.25.1.1.7

7.1.7. Uso de la extensión Policy Constraints

Según lo establecido en la DPC de ANF AC.

7.1.8. Sintaxis y semántica de los calificadores de política

Según lo establecido en la DPC de ANF AC.

7.1.9. Semántica de procesamiento de la extensión critical Certificate Policies

Según lo establecido en la DPC de ANF AC.

7.2. Perfil CRL

Según lo establecido en la DPC de ANF AC.

7.3. Perfil OCSP

Según lo establecido en la DPC de ANF AC.

8. Auditorías de cumplimiento y otros controles

8.1. Frecuencia de las auditorías

Según lo establecido en la DPC de ANF AC.

8.2. Cualificación del auditor o evaluador

Según lo establecido en la DPC de ANF AC.

8.3. Relación entre el auditor y la autoridad auditada

Según lo establecido en la DPC de ANF AC.

8.4. Aspectos cubiertos por la evaluación

Según lo establecido en la DPC de ANF AC.

8.5. Acciones a emprender como resultado de la detección de deficiencias

Según lo establecido en la DPC de ANF AC.

9. Otras cuestiones legales y de actividad

9.1. Tarifas

Según lo establecido en la DPC de ANF AC.

9.2. Responsabilidades económicas

Según lo establecido en la DPC de ANF AC.

9.3. Confidencialidad de la información comercial

Según lo establecido en la DPC de ANF AC.

9.4. Protección de la información personal

Según lo establecido en la DPC de ANF AC.

9.5. Derechos de propiedad intelectual

Según lo establecido en la DPC de ANF AC.

9.6. Obligaciones y garantías

Según lo establecido en la DPC de ANF AC.

9.7. Exención de garantía

Según lo establecido en la DPC de ANF AC.

9.8. Limitaciones de responsabilidad

Según lo establecido en la DPC de ANF AC.

9.9. Indemnizaciones

Según lo establecido en la DPC de ANF AC.

9.10. Periodo de validez y terminación

Según lo establecido en la DPC de ANF AC.

9.11. Avisos y comunicaciones individuales con los participantes

Según lo establecido en la DPC de ANF AC.

9.12. Modificaciones o cambios en las especificaciones

Según lo establecido en la DPC de ANF AC.

9.13. Disposiciones para la resolución de conflictos

Según lo establecido en la DPC de ANF AC.

9.14. Normativa aplicable

Según lo establecido en la DPC de ANF AC.

9.15. Cumplimiento de la normativa aplicable

Según lo establecido en la DPC de ANF AC.

9.16. Disposiciones diversas

Según lo establecido en la DPC de ANF AC.

9.17. Otras disposiciones

Según lo establecido en la DPC de ANF AC.