Certificados SSL y Sede Electrónica

Política de Certificación

SSL DV, OV, EV, QWAC y PSD2

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

902 902 172

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)

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

Web: www.anf.es

ÍNDICE

1. INTRODUCCIÓN

1.1. Visión General

Esta Política de Certificación (PC) define los requisitos de procedimiento y operacionales que ANF AC lleva a cabo para la emisión y gestión de certificados de Servidor Seguro SSL de acuerdo con *Certification Authority/Browser Forum* (CA/B Forum) *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificate* (en adelante, Baseline Requirements), certificados de Servidor Seguro SSL con validación extendida de acuerdo con *CA/B Forum Guidelines for Extended Validation Certificates* (en adelante, EV Guidelines) y Certificados de Autenticación de Sitio Web Cualificados (QWAC) de acuerdo con el Reglamento (UE) 910/2014 (en adelante, el Reglamento eIDAS).

El propósito de esta PC es detallar y completar lo que se define genéricamente en la Declaración de Prácticas de Certificación (DPC) de ANF AC (OID 1.3.6.1.4.1.18332.1.9.1.1) para este tipo de certificados y especificar las políticas que ANF AC adopta para cumplir con las versiones actuales de Las siguientes políticas, directrices y requisitos:

- Artículo 45 del Reglamento (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.
- Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros
- ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate Profile for web site certificates,
- ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Públicor. El Ministerio de Hacienda y Administraciones Públicas define el perfil del certificado de sede electrónica.
- CA/B Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* situados en https://cabforum.org/baseline-requirements-documents ,
- CA/B Forum *Guidelines for Extended Validation Certificates* situados en https://cabforum.org/extended-validation ,
- CA/B Forum *Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates*,
- Microsoft Trusted Root Program Requirements,
- Mozilla Root Store Policy, and
- Google's Certificate Transparency project.

Con respecto a los Certificados de Servidor SSL/TLS o los Certificados de Firma de Código, en el caso de darse alguna inconsistencia entre esta PC y los requisitos y directrices anteriores, los requisitos y las directrices de CA/B Forum tomarán prioridad.

Esta PC es solo uno de los varios documentos que rigen la PKI de ANF AC. Otros documentos importantes incluyen la Declaración de Prácticas de Certificación, el acuerdo de la Autoridad de Registro, los contratos de suscripción, los términos y condiciones, las políticas de privacidad y la adenda de ANF AC. Estas políticas y declaraciones complementarias están disponibles para los usuarios correspondientes o los terceros que confían.

En conformidad con el marco RFC 3647 CP/CPS, esta PC se divide en nueve partes que cubren los controles de seguridad y las prácticas y procedimientos para el certificado o los servicios de sellado de tiempo dentro de la PKI de ANF AC. En los apartados y subapartados ya cubiertos por la DPC de ANF AC encontrará la declaración "Definido en la DPC de ANF AC".

Esta PC 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.

1.1.1. Descripción de los certificados

ANF AC, en el marco de su servicio de certificación electrónica, emite certificados técnicos de tipo:

Servidor Seguro SSL	Sede Electrónica
Validación de Dominio (DV)	Nivel meido y alto
Validación de Organización (OV)	Validación Extendida, nivel medio y alto
Validación Extendida (EV) - Qualified Website Authentication (QWAC)	
Validación Extendida (EV) QWAC for PSD2 (QWAC PSD2)	

Certificados de Servidor Seguro SSL:

- **Certificado de SSL Validación de Organización (DV)**
  Este certificado será utilizado para la identificación de la titularidad del dominio que alberga el sitio web, proporcionando una garantía razonable al usuario de un navegador de Internet. El DV Wildcard contiene un “comodín” en el nombre de host (ej.: *.frater.com). Se emiten según los requerimientos de CAB Forum para los certificados DV como se especifica en los Baseline Requirement y ETSI EN 319 411-1. La validez de estos certificados puede ser de hasta 397 días.

- **Organization Validated Secure Server SSL Certificate (OV)**
  Este certificado será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía razonable al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado. El OV Wildcard contiene un “comodín” en el nombre de host (ej.: *.frater.com). Se emiten según los requerimientos de CA/B Forum Baseline Requirements y en cumplimiento ETSI EN 319 411-1. La validez de estos certificados puede ser de hasta 397 días.

- **SSL Cualificado Validación Extendida (EV) – Certificado Cualificado de Autenticación de Sitio Web (QWAC)**
  Certificado Secure Server SSL con Validación Extendida, en cumplimiento con el Reglamento eIDAS. Este certificado es emitido con la consideración de cualificado según el Reglamento eIDAS, será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía robusta al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado. Cumple con los requerimientos establecidos en ETSI EN 319 412-4 y en CA/B Forum EV Guidelines. Los certificados emitidos con Extended Validation, tienen un periodo máximo de validez 397 días. Este tipo de certificado solo puede ser expedido a personas jurídicas.

Además de las utilidades proporcionadas por el certificado SSL, la Validación Extendida (EV) tiene como objetivo proporcionar un mejor nivel de autenticación de las organizaciones para asegurar las transacciones en sus sitios web. El objetivo de los Certificados SSL EV, es su utilización en protocolos TLS / SSL con la finalidad de garantizar la validez de la constitución de la organización identificada en el certificado, evitando casos de *phishing* u otros casos de fraude de identidad en línea.

- **Qualified Website Authentication Certificate para PSD2 (QWAC PSD2)**
  Este certificado es emitido con la consideración de cualificado según Reglamento eIDAS, es un QWAC *(ETSI EN 319 412-4 y CA/B Forum EV Guidelines)* emitido en conformidad con la ETSI TS 119 495 y en cumplimineto con los *Regulatory Technical Standards (RTS)* del Reglamento Delegado (UE) 2018/389 de la Comisión, por el que se complementa la Directiva (UE) 2015/2366, y el Real Decreto-ley 19/2018 de España, respetando las directrices establecidas por la Autoridad Nacional Competente de servicios de pago. ANF AC garantiza un procedimiento de identificación de la titularidad del dominio y acreditación de la organización titular del mismo, equivalente al procedimiento seguido para la emisión de certificados con Validación Extendida (EV). Los certificados emitidos con Extended Validation, tienen un periodo máximo de validez de 397 días.

Certificado de Sede Electrónica *(de acuerdo a la ley 40/2015)***:**

- **Certificado Cualificado de Sede Electrónica con Validación Extendida (EV)**
  En el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ANF AC emite certificados del tipo sede electrónica. Se emiten según la política de ETSI EN 319 411-2, en conformidad con los EV Guidelines de CA/B Forum y el perfil de certificado de sede definido por el Ministerio de Hacienda y Administraciones Públicas. Son certificados cualificados de autenticación web conforme al Reglamento eIDAS, identifican a la Administración Pública, órgano o entidad administrativa titular de la sede. El fin de este certificado es establecer comunicaciones de datos vía TLS/SSL en servicios y aplicaciones informáticas, proporcionar autenticación de la Administración Pública, órgano o entidad administrativa para asegurar las transacciones en sus sitios Web evitando casos de *phishing* u otros casos de fraude de identidad on-line.

  La validez de estos certificados puede ser de hasta 397 días.
  Los certificados del tipo Sede Electrónica, seguirán las definiciones establecidas por la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) en su documento “Perfiles de certificados electrónicos” de abril de 2016. Se definen dos niveles de aseguramiento:
  a. **Nivel medio / sustancial:**
     Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para la mayoría de aplicaciones. El riesgo previsto por este nivel es apropiado para acceder a aplicaciones clasificadas según el ENS en los niveles de Integridad y Autenticidad como de riesgo bajo o medio.
  b. **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 es apropiado para acceder a aplicaciones clasificadas según el ENS en los niveles de Integridad y Autenticidad como de riesgo alto.

1.2. Nombre del documento e identificación

Nombre del documento	Política de Certificación de Certificados SSL y Sede Electrónica
Versión	3.3.1
Estado de la política	APROBADA
OID	1.3.6.1.4.1.18332.55.1.1
Fecha de publicación	08/01/2021
DPC relacionada	Declaración de Prácticas de Certificación (DPC) de ANF AC
Ubicación	https://www.anf.es/en/

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

1.2.1. Revisiones

Versión	Cambios	Aprobación	Publicación
3.3.1.	Actualización banda de acreditaciones, corrección de faltas y acrónimos.	08/01/2020	08/01/2020
3.3.	Correcciones para alinearse con Mozila's Root Store Policy	09/11/2020	09/11/2020
3.2.1	Actualización de enlaces de Reportar incumplimiento o uso indebido.	30/10/2020	30/10/2020
3.2.	Actualización de los BR 1.7.3. y EVG 1.7.4. Cambios en las razones para revocar un certificado de suscriptor y aclaración en el apartado 6.1.2.	10/10/2020	10/10/2020
3.1.	Actualización de los BR 1.7.2. Cambio menor, Se especifica el no uso del método 3.2.2.4.10	20/09/2020	20/09/2020
3.0	Actualización de los BR 1.7.1. y EVG 1.7.3. Cambio período de validez máximo a 397 dias.	10/08/2020	10/08/2020
2.10	Actualización de los BR 1.7.0. Sin cambios.	15/04/2020	15/04/2020
2.9	Revisión actualización BR 1.6.8 y 1.6.9 y EVG 1.7.2. Sin cambios. ANF AC no emite certificados .onion	25/02/2020	25/02/2020
2.8	Merjora en la adaptación a RFC 3647. Actualización de los BR *1.6.6.* y retirada del certificado SSL IV	19/07/2019	19/07/2019
2.7	Actualización para aclarar y cumplir con los requisitos de políticas de PSD2 establecidos en ETSI TS 119 495	28/03/2019	28/03/2019
2.6	Inclusión de certificados PSD2	30/01/2019	30/01/2019
2.5	Revisión anual	15/01/2019	15/01/2019
2.4	Revisión anual	22/02/2018	22/02/2018
2.3	Actualización para adaptarse y cumplir con los requisitos del Reglamento eIDAS y los EV Guidelines	27/02/2017	27/02/2017
2.2	Revisión y actualización para aclaración	04/11/2016	04/11/2016
2.1	Actualización para una mejora en la adaptación a los Baseline Requirements	25/06/2016	25/06/2016
2.0	Creación del documento	10/07/2015	10/07/2015

1.2.2. OIDs

A fin de identificar los certificados, se ha asignado los siguientes identificadores de objeto (OID)

Para los certificados técnicos emitidos por la jerarquía **ANF Global Root CA,** con fecha de caducidad **2036**:

Servidor Seguro SSL	DV	Soft. Criptográfico	1.3.6.1.4.1.18332.55.1.1.1.22
	OV		1.3.6.1.4.1.18332.55.1.1.7.22
Servidor Seguro SSL Cualificado *(QWAC)*	PSD2	Soft. Criptográfico	1.3.6.1.4.1.18332.55.1.1.8.22
	EV Cualificado *(QWAC)*		1.3.6.1.4.1.18332.55.1.1.2.22
Sede Electrónica EV	Nivel Medio	Soft. Criptográfico	1.3.6.1.4.1.18332.55.1.1.5.22
	Nivel Alto	Token HSM	1.3.6.1.4.1.18332.55.1.1.6.22

Para los certificados técnicos emitidos por la jerarquía **ANF Secure Server Root CA**:

Servidor Seguro SSL	DV	Soft. Criptográfico	1.3.6.1.4.1.18332.55.1.1.1.322
	OV		1.3.6.1.4.1.18332.55.1.1.7.322
Servidor Seguro SSL Cualificado *(QWAC)*	PSD2	Soft. Criptográfico	1.3.6.1.4.1.18332.55.1.1.8.322
	EV Cualificado *(QWAC)*		1.3.6.1.4.1.18332.55.1.1.2.322
Sede Electrónica EV	Nivel Medio	Soft. Criptográfico	1.3.6.1.4.1.18332.55.1.1.5.322
	Nivel Alto	Token HSM	1.3.6.1.4.1.18332.55.1.1.6.322

En la extensión CertificatePolicies (2.5.29.32), podrá incluirse, como medio de afirmación del cumplimiento de esta Política con los criterios adoptados por CA/B Forum y ETSI, los siguientes OID:

	CA/B Forum	**ETSI**
SSL DV	2.23.140.1.2.1	DVCP *(Domain Validation Certificate Policy)*: 0.4.0.2042.1.5
SSL OV	2.23.140.1.2.2	OVCP *(Organizational Validation Certificate Policy):* 0.4.0.2042.1.6
EV Cualificado *(QWAC)*	2.23.140.1.1	QCP-W *(certificate policy for EU-certified website authentication certificates):* 0.4.0.194112.1.4
QWAC PSD2	2.23.140.1.1	QCP-W *(certificate policy for EU-certified website authentication certificates):* 0.4.0.194112.1.4 QCP-W-PSD2 certificate policy for EU qualified PSD2 website authentication certificates 0.4.0.19494.3
QWAC Persona Física	2.23.140.1.2.3	QCP-W *(certificate policy for EU-certified website authentication certificates):* 0.4.0.194112.1.4

Además, como medio de afirmación del cumplimiento de los requerimientos establecidos en el ámbito de la Administración General del Estado de España y de sus organismos públicos, en la extensión CertificatePolicies (2.5.29.32), se incluirá en PolicyInformation en el caso de certificados de Sede Electrónica:

	CA/B Forum	ETSI	Administración Española
Nivel Alto Sede Electrónica EV	2.23.140.1.1	QCP-W *(certificate policy for EU-certified website authentication certificates):* 0.4.0.194112.1.4	2.16.724.1.3.5.5.1
Nivel Medio Sede Electrónica EV	2.23.140.1.1	QCP-W *(certificate policy for EU-certified website authentication certificates):* OID 0.4.0.194112.1.4 QCP-W-PSD2 certificate policy for EU qualified PSD2 website authentication certificates 0.4.0.19494.3	2.16.724.1.3.5.5.2

1.3. Participantes de la PKI

De forma general, los participantes de la PKI están definidos en la DPC de ANF AC.

Se requieren los siguientes roles de Suscriptor para la emisión de un certificado EV.

1. **Solicitante de certificado**: persona física que presenta la solicitud de certificado de EV y tiene suficientes poderes de representación de la organización o entidad. Puede ser el propio Suscriptor, empleado del suscriptor, un agente autorizado que tiene autoridad expresa para representar al suscriptor, o un tercero (como un ISP o una compañía de hosting) que completa y envía una solicitud de Certificado EV en nombre del Suscriptor.
2. **Aprobador de certificados**: persona física que aprueba la Solicitud de certificado de EV, que es el suscriptor, empleado por el Solicitante o un agente autorizado que tiene autoridad expresa para representar al suscriptor para (i) actuar como solicitante de certificado y autorizar a otros los empleados o terceros actúen como solicitantes de certificados y (ii) para aprobar las solicitudes de certificado de EV enviadas por otros solicitantes de certificados.
3. **Firmante del contrato**: persona física autorizada para firmar el Contrato de suscripción aplicable al Certificado EV solicitado, que puede ser el propio suscriptor, empleado por el suscriptor o un agente autorizado que tiene la autoridad expresa para representar al suscriptor, y que tiene autoridad suficiente para firmar Contratos de suscripción.
4. **Representante del suscriptor**: en el caso de que la CA y el Suscriptor estén afiliados, los Términos de uso aplicables al Certificado EV solicitado deben ser reconocidos y aceptados por un Representante del suscriptor autorizado. Un Representante del suscriptor es una persona física que puede ser el suscriptor, empleado del suscriptor o un agente autorizado que tiene autoridad expresa para representar al suscriptor, y que tiene autoridad en nombre del suscriptor para reconocer y aceptar los Términos de uso.

1.4. Uso del certificado

1.4.1. Usos apropiados

El Certificado emitido bajo esta Política puede ser utilizado con los siguientes propósitos:

- Identificación del DNS. El Certificado emitido bajo la presente Política permite identificar y vincular una determinada DNS *–Domain Name System-* (en español: sistema de nombre de Dominio) a la entidad titular de ese dominio, que es el suscriptor del certificado.

- La encriptación de las comunicaciones entre el usuario y el sitio web, facilitando el intercambio de las claves de cifrado necesarias para el cifrado de la información a través de Internet.

1.4.2. Usos prohibidos

No se permiten otros usos distintos de los establecidos en esta Política y en la DPC de ANF AC.

1.5. Administración de la política

ANF AC tutela y supervisa que esta PC sea compatible y esté en coherencia con el resto de documentos que ha elaborado. Este documento es periódicamente revisado, al menos una vez al año y siempre que se produzcan novedades legales o normativas que ocasionen cambios en los procedimientos. Toda la documentación está a libre disposición de usuarios y terceros que confían en https://www.anf.es

1.5.1. Organización que administra el documento

La Junta Rectora de la PKI es responsable de la administración de esta PC y del resto de Políticas y Declaración de Prácticas de Certificación de ANF AC. La fecha de publicación es la fecha de entrada en vigor.

Departamento	Junta Rectora de la PKI
Email	juntapki@anf.es
Dirección	Paseo de la Castellana, 79
Región	Madrid
Código Postal	28046
Número de teléfono	902 902 172 (Llamadas desde España) Internacional (+34) 933 935 946

1.5.2. Persona de contacto

Departamento	Departamento Legal
Correo electrónico 1	soporte@anf.es
Correo electrónico 2	mcmateo@anf.es
Dirección	Paseo de la Castellana, 79
Localidad	Madrid
Código Postal	28046
Número de teléfono	902 902 172 (Llamadas desde España) Internacional (+34) 933 935 946

1.5.2.1. Persona de contacto para revocaciones

Los suscriptores, los terceros que confían, los proveedores de software de aplicación y otras terceras partes pueden enviar informes de problemas sobre certificados informando a ANF AC AC de una causa razonable para revocar un certificado:

- A través de la persona de contacto reseñada en esta sección 1.5.2.
- Directamente rellenando el siguiente formulario web https://www.anf.es/sat-incumplimiento-uso-indebido/
- Cualquier otro método especificado en la sección 4.9.3. de este documento.

Esto incluye denunciar un supuesto compromiso de clave privada, uso incorrecto de certificados, otros tipos de fraude, compromiso, uso indebido, conducta inapropiada o cualquier otro asunto relacionado con los certificados o la PKI de ANF AC.

1.5.3. Persona que determina la idoneidad de las políticas a la DPC

ANF AC determina la idoneidad y aplicabilidad de esta PC y la conformidad de esta PC a la DPC en función de los resultados y las recomendaciones recibidas de un auditor independiente (ver sección 8). ANF AC también es responsable de evaluar y actuar sobre los resultados de las auditorías de cumplimiento.

1.5.4. Procedimiento de aprobación de políticas

Según lo definido en la DPC de ANF AC.

1.6. Definiciones y acronimos

Las definiciones y acrónimos se definen en la DPC de ANF AC, excepto que se defina de otra manera en este documento:

1.6.1. Definiciones

Proveedor de software de aplicación: un proveedor de software de navegador de Internet u otro software de aplicación de usuario de confianza que muestra o utiliza Certificados e incorpora certificados raíz.

Carta de atestación: una carta que acredite que la información del sujeto es correcta y está escrita por un notario, abogado, funcionario del gobierno u otro tercero de fe pública.

CAA: De RFC 6844 (http: tools.ietf.org/html/rfc6844): “El Registro de Recursos DNS de Autorización de Autoridad de Certificación (CAA) permite que un titular de nombre de dominio DNS especifique las Autoridades de Certificación (CA) autorizadas para emitir certificados para ese dominio. "La publicación de los Registros de Recursos de la CAA permite a una Autoridad de Certificación pública implementar controles adicionales para reducir el riesgo de que se pierda el certificado involuntariamente".

Informe de problemas con el certificado: reclamo por presunto compromiso con la clave, mal uso del certificado u otros tipos de fraude, compromiso, mal uso o conducta inapropiada relacionada con los certificados.

Documento de Autorización de Dominio: Documentación proporcionada por, o la documentación de una CA de una comunicación con, un Registrador de Nombres de Dominio, el Registrante de Nombres de Dominio, o la persona o entidad que figura en WHOIS como el Registrante de Nombres de Dominio (incluido cualquier registro privado, anónimo o proxy) servicio) que acredite la autoridad de un solicitante para solicitar un certificado para un espacio de nombres de dominio específico.

Contacto de dominio: el Registrante de nombre de dominio, el contacto técnico o el contrato administrativo (o el equivalente bajo un ccTLD) como se indica en el registro de WHOIS del Nombre de dominio base o en un registro SOA de DNS, o como se obtiene a través del contacto directo con el Nombre de dominio Registrador.

Nombre de dominio: la etiqueta asignada a un nodo en el sistema de nombres de dominio.

Espacio de nombres de dominio: el conjunto de todos los posibles nombres de dominio que están subordinados a un solo nodo en el sistema de nombres de dominio.

Registrador de nombres de dominio: a veces se lo denomina "propietario" de un nombre de dominio, pero más adecuadamente las personas o entidades registradas con un registrador de nombres de dominio tienen derecho a controlar cómo se usa un nombre de dominio, como como la persona natural o entidad legal que figura como el "Registrante" por WHOIS o el Registrador de nombres de dominio.

Registrador de nombres de dominio: una persona o entidad que registra nombres de dominio bajo los auspicios de o de acuerdo con: (i) la Corporación de Internet para Nombres y Números Asignados (ICANN), (ii) una autoridad / registro nacional de Nombres de Dominio, o (iii) un Centro de información de la red (incluidos sus afiliados, contratistas, delegados, sucesores o cesionarios).

Certificado de Validación de Dominio (DVC): certificado que no contiene información validada de identidad para el sujeto, solo identifica al sujeto por su nombre de dominio

Certificado EV: un certificado que contiene información sobre el sujeto especificado en los EV Guidelines y que ha sido validado de acuerdo con los EV Guidelines de CA/B Forum.

Certificado de validación organizacional (OVC): certificado que incluye información validada de identidad de organización del sujeto.

Nombre de dominio completo: un nombre de dominio que incluye las etiquetas de todos los nodos superiores en el sistema de nombres de dominio de Internet.

Persona principal: un individuo de una Organización privada, Entidad gubernamental o Entidad comercial que sea propietario, socio, miembro administrador, director o funcionario, según lo identifique su título de empleado, o un empleado, contratista o agente autorizado por tal entidad u organización para llevar a cabo negocios relacionados con la solicitud, emisión y uso de Certificados EV.

Certificado de confianza pública: un certificado en el que se confía en virtud del hecho de que su certificado raíz correspondiente se distribuye como un ancla de confianza en un software de aplicación ampliamente disponible.

Fuente de información gubernamental Cualificada: Una base de datos mantenida por una entidad gubernamental que cumple con los requisitos de la Sección 11.11.6 de los EV Guidelines.

Fuente de información independiente calificada: Una base de datos actualizada, actualizada y disponible al público, diseñada con el propósito de proporcionar con precisión la información para la cual se la consulta, y que generalmente se reconoce como una fuente confiable de dicha información.

Nombre de dominio registrado: un nombre de dominio que se ha registrado con un registrador de nombres de dominio.

Carta del contador verificado: un documento que cumple con los requisitos especificados en la Sección 11.11.2 de los EV Guidelines.

Opinión legal verificada: Un documento que cumple con los requisitos especificados en la Sección 11.11.1 de los EV Guidelines.

Carta profesional verificada: una carta del contador verificado o opinión legal verificada.

1.6.2. Acrónimos

CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
DBA	Doing Business As
DNS	Domain Name System

FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPA	Chartered Professional Accountant
CSO	Chief Security Officer
EV	Extended Validation
gTLD	Generic Top-Level Domain
IFAC	International Federation of Accountants
ISP	Internet Service Provider
QGIS	Qualified Government Information Service
UTC(k)	National realization of Coordinated Universal Time
DVC	Domain Validation Certificate
EVC	Extended Validation Certificate
OVC	Organization Validation Certificate
RDE	Responsible de Dictámenes de Emisión
ARR	Autoridad de Registro Reconocida
OVP	Oficina de Verificación Presencial

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

2.1. Repositorios

Según lo definido en la DPC de ANF AC.

2.2. Publicación de información sobre certificación

Según lo definido en la DPC de ANF AC.

Específico para los Certificados QWAC PSD2: La Autoridad Nacional Competente puede solicitar información sobre los certificados que contienen un número de autorización de un Proveedor de Servicios de Pago (PSP) asignado por esa institución. ANF AC informará sobre los certificados emitidos de acuerdo con las disposiciones de cada repositorio.

En el ámbito del proyecto Google Certificate Transparency (CT), los certificados emitidos con la calificación EV (Extended Validation) se publicarán en diferentes operadores de CT Log, para cumplir con la propuesta RFC 6962 Certificate Transparency.

2.3. Momento y frecuencia de publicación

Según lo definido en la DPC de ANF AC.

2.4. Controles de acceso a los repositorios

Según lo definido en la DPC de ANF AC.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Nombres

3.1.1. Tipos de nombres

Según lo definido en la DPC de ANF AC.

ANF AC actualmente no emite certificados a un Nombre de dominio con .onion.

3.1.2. Necesidad de que los nombres sean significativos

Todos los certificados del tipo Servidor Seguro SSL y Servidor Seguro SSL EV contienen un nombre distintivo (DN) que identifica al dominio DNS y a la persona u organización titular del mismo, de acuerdo con lo previsto en la Recomendación ITU-T X.501, contenido en el campo Subject.

3.1.3. Anonimato o seudonimia de los suscriptores

No permitido.

3.1.4. Normas para interpretar diferentes formas de nombre

Según lo definido en la DPC de ANF AC.

3.1.5. Unicidad de los nombres

El certificado se emitirá con el nombre completo al que responda el servicio que se va a dotar con características SSL. Este nombre debe ser único en la red. No se aceptarán nombres parciales.

3.1.6. Reconocimiento, autenticación, y rol de marcas registradas

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

Para EV SSL, ANF AC no incluye, en un atributo de OU, un nombre, DBA, nombre comercial, marca registrada, dirección, ubicación u otro texto que se refiera a una persona física o entidad legal específica a menos que esta información haya sido verificada de acuerdo con los EV Guidelines.

3.2. Validación inicial de la identidad

Esta sección describe los procedimientos llevados a cabo con carácter general para la validación de identidad. Los procesos de verificación y validación de la solicitud que se aplican a cada tipo de certificado se especifican en la sección 4.2.1 de esta PC.

3.2.1. Método para demostrar la posesión de la clave privada

Según lo definido en la DPC de ANF AC.

3.2.2. Autenticación de la identidad de una Organización y Dominio

ANF AC inspecciona cualquier documento usado en esta sección para detectar alteración o falsificación.

3.2.2.1. Identidad de la Organización

En caso de que el certificado deba incluir los datos de una organización, ANF AC verificará la identidad y la dirección de la organización y que la dirección es la dirección de existencia u operación del solicitante, de acuerdo con la sección 3.2.2.1 de los Baseline Requirements. Para los certificados EV se publica el listado de fuentes de verificación en el repositorio legal de la web de ANF AC.

Se requerirá lo siguiente:

- **Cédula de identificación fiscal (CIF) de la entidad**

Además, según forma jurídica, ANF AC verificará la identidad y dirección del Suscriptor mediante:

- Las sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Mercantil acreditarán la válida constitución mediante la aportación de:
  - Para solicitudes de certificados SSL OV, nota simple del Registro Mercantil relativa a los datos de constitución y cargos vigentes de administración de la entidad.
  - Para solicitudes de certificados SSL EV, original o copia auténtica del Registro Mercantil relativo a los datos de constitución y cargos vigentes de administración de la entidad.
- Las asociaciones, fundaciones y cooperativas acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado del registro público donde consten inscritas, relativo a su constitución.
- Las sociedades civiles y demás personas jurídicas aportarán original o copia auténtica del documento público que acredite su constitución de manera fehaciente.
- Las Administraciones Públicas y entidades pertenecientes al sector público:
  - Entidades cuya inscripción sea obligatoria en un Registro acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado relativo a los datos de constitución y personalidad jurídica de las mismas.
  - Entidades creadas por norma, aportarán referencia a la norma de creación.

Como opción alternativa, se consultará una base de datos de terceros que se actualice periódicamente y se considere una fuente de datos fiable. Se entiende que una fuente de este tipo es una base de datos utilizada para verificar la información sobre la identidad de las organizaciones, reconocida entre las empresas comerciales y las administraciones públicas como una fuente fiable y creada por un tercero diferente al solicitante. Como por ejemplo einforma, DUN & BRADSTREET o el Identificador de entidad legal (LEI).

Si la ARR o el RDE lo consideran necesario, pueden solicitar documentos adicionales para cotejar la fiabilidad de la información, como, por ejemplo, facturas recientes de servicios públicos y extractos de cuenta bancaria. Si la ARR o el RDE conocen de forma personal al suscriptor, deberán emitir y firmar una Declaración de Identidad[1].

3.2.2.2. Nombre comercial (DBA)

ANF AC no permite el uso de DBA o d/b/a.

3.2.2.3. Verificación de País

Si se incluye el campo subject:countryName, ANF AC verificará el país asociado con el Sujeto mediante el método identificado en la Sección 3.2.2.1 o, alternativamente, mediante el ccTLD del Nombre de dominio solicitado.

3.2.2.4. Validación de Autorización y Control de Dominio

[1] *Consiste en una declaración formal jurada, en la que el declarante manifiesta que conoce de forma personal y directa a una determinada persona física o a una persona jurídica. Además, hace constar, hasta donde alcance su conocimiento directo, que ha verificado los datos de filiación reseñados en el Formulario de Solicitud: dirección, teléfono y correo electrónico, y que son ciertos.*
La Declaración de Identidad incorpora la identidad del declarante, su cédula de identidad, la información que ha sido validada, la fecha y hora de la verificación, la firma del declarante y los apercibimientos legales correspondientes en caso de incurrir en perjurio.
En el caso de intervención de Notario Público, se requerirá la legitimación de firma del suscriptor en a solicitud de expedición de un certificado (LFE 59/2003, Art. 13.1).

ANF AC confirma que, antes de la emisión, ha validado el Nombre de dominio completo (FQDN) que figura en el Certificado utilizando al menos uno de los métodos siguientes, en conformidad con la sección 3.2.2.4 de los Baseline Requirements:

Email, Fax, SMS, o Correo Postal al Contacto de Dominio *(3.2.2.4.2)*	Envío de valor aleatorio por correo electrónico, fax, SMS o correo postal y recepción de una confirmación que contenga dicho valor aleatorio. Dicha dirección deberá estar identificada como un contacto de dominio en los registros de WHOIS "*registrant*", "*technical*", o "*administrative*". Las direcciones de correo electrónico están limitadas a "*admin*", "*administrador*", "*webmaster*", "*hostmaster*" y "*postmaster*". Este valor aleatorio será único para cada envío y tendrá un periodo de validez de 30 días desde su creación.
Correo electrónico construido al Contacto de Dominio *(3.2.2.4.4)*	Envío de un correo electrónico a una o más direcciones creadas usando *'admin'*, *'administrador'*, *'webmaster'*, *'hostmaster'* o *'postmaster'* como parte local, seguido de atsign ("@"), seguido del ADN, incluyendo un valor aleatorio (único para cada correo electrónico, y con un periodo de validez de 30 días desde su creación), y recepción de una confirmación que contenga dicho valor aleatorio,
Contacto telefónico con el Contacto de Dominio *(3.2.2.4.15)*	Llamada al número de teléfono del contacto del dominio y obtención de una confirmación para validar el ADN. Cada llamada telefónica puede confirmar el control de varios ADN, siempre que el mismo número de teléfono de contacto del dominio esté listado para cada ADN, que se verifique y proporcione una respuesta de confirmación para cada ADN.

ANF AC NO utiliza los métodos de validación de dominio retirados, especificados en el apartado 3.2.2.4.1, apartado 3.2.2.4.3, apartado 3.2.2.4.5, apartado 3.2.2.4.6, apartado 3.2.2.4.9, apartado 3.2.2.4.10 y apartado 3.2.2.4.11 de los CA/B Forum Baseline Requirements. ANF AC NO utiliza el método descrito en el apartado 3.2.2.4.10 de los Baseline Requirements ya que presenta vulnerabilidades importantes.

ANF AC realiza las tareas de validación del dominio y no las delega a terceras partes.

ANF AC mantiene un registro de qué método de validación de dominio, incluido el número de versión de BR relevante, se utilizó para validar cada dominio.

ANF AC NO emite certificados que contengan un nuevo gTLD bajo consideración por ICANN, o Nombres de dominio Internos *(Internal Domain Names)*.

Se verificará que el dominio no consta entre aquellos listados como de riesgo, en Google Safe Browsing Lists o en la lista de phishing de Miller Smiles.

Asimismo, para dominios asociados a nombres que pueden crear en terceros que confían por:

- Confusión de identidad o actividad.

No se autorizará emisión de certificado cuando el nombre del dominio pueda crear confusión respecto a la verdadera actividad del suscriptor (p. ej.www.bancoprogreso.com, cuando la actividad del suscriptor no se corresponde al de una entidad financiera).

No se autorizará emisión de certificado cuando el nombre del dominio pueda crear confusión respecto a la verdadera actividad del suscriptor (p. ej.www.bancoprogreso.com, cuando la actividad del suscriptor no se corresponde al de una entidad financiera).

- Marcas especialmente relevantes.

En caso de dominio asociado a marca especialmente relevante, se comprobará el Registro de Patentes y Marcas. Cuando el nombre del dominio este asociado a una marca de especial relevancia y conocimiento público se verificará si el propietario de la marca corresponde al suscriptor. En caso negativo, el RDE solicitará aclaración al suscriptor si tiene algún tipo de autorización acreditativa.

No se autorizará emisión de certificado cuando el nombre esté asociado a una marca relevante de la que no es propietario el suscriptor del dominio, ni tiene autorización del propietario de la marca, dado que puede causar confusión a terceros que confían (p.ej., www.chanel.zn, www.cocacola.eu, etc.)

3.2.2.5. Validación de Dominio Wildcard

En el caso de los certificados SSL DV y SSL OV, se permitirá Wildcard en subdominios o nombres de host, pero no en dominios de nivel superior (TLD) o en el nombre de dominio.

La entidad suscriptora deberá poder demostrar su legítimo control del dominio completo, en caso contrario se rechazará la solicitud. Por ejemplo, no se pueden emitir *.co.uk, *.local o ejemplo.*, pero si *.ejemplo.com a la empresa Ejemplo S.A.

La determinación de lo que es "*registry-controlled*" en comparación con la parte registrable de un CountryCode Top-Level Domain Namespace no está estandarizada en el momento de la redacción de los Baseline Requirements y no es una propiedad del DNS en sí. La mejor práctica actual es consultar una "*lista de sufijos públicos*", como http://publicsuffix.org/ (PSL), y recuperar una copia nueva con regularidad. Si usa dicha lista, ANF AC consultará la sección "DOMINIOS DE ICANN" únicamente, no la sección "DOMINIOS PRIVADOS". Esta lista se actualiza regularmente para contener nuevos gTLD delegados por la ICANN, que se enumeran en la sección "DOMINIOS DE LA ICANN". ANF AC puede emitir un Wildcard al Registrante de un gTLD completo, siempre que el control de todo el espacio de nombres se demuestre de manera adecuada.

3.2.3. Autenticación de la identidad de persona física

ANF AC requerirá al solicitante del certificado, persona física, la siguiente documentación:

- **DNI, NIE o Pasaporte,** en caso de ciudadanos nacionales o miembros de la Unión Europea. En caso de ciudadanos extranjeros extracomunitarios, se requerirá: Pasaporte; tarjeta de residencia, permiso de trabajo, en su caso. Dicho documento deberá incluir una fotografía permita cotejar la identidad de la persona compareciente. En caso de escasa nitidez, se podrá solicitar otro documento oficial que incorpore fotografía, p.ej., licencia de conducir.

- **Suficiente Poder de Representación**
  Además de los representantes legales, se aceptarán representantes voluntarios cuando demuestren poderes suficientes para realizar actos legales o celebrar contratos en nombre de la entidad.

ANF AC inspeccionará los documentos para detectar cualquier indicio de alteración o falsificación y verificará la dirección del suscriptor utilizando el mismo DNI, NIE o Pasaporte.

ANF AC verificará la solicitud de certificado con el solicitante utilizando un método confiable de comunicación. Para los certificados con la consideración de cualificados por el Reglamento eIDAS, se requerirá la verificación presencial de la identidad del solicitante, pudiendo esta ser evitada en caso de legitimación de la firma del contrato ante notario o en caso de firma cualificada en el contrato y solicitud.

3.2.4. Información no verificada sobre el suscriptor

Los certificados SSL DV no incluyen una identidad de organización verificada.

3.2.5. Validación de las facultades de representación

ANF AC toma medidas razonables para determinar que una solicitud realizada en nombre de una Organización es legítima y está debidamente autorizada. ANF AC verificará que el representante legal solicitante posee poderes de representación suficientes, de acuerdo con la sección 3.2.3 de esta PC.

En el caso de los certificados SSL OV, ANF AC verificará la autenticidad de la solicitud utilizando un método fiable de comunicación con el representante, como se define en los Baseline Requirements.

Para certificados EV, como se especifica en los EV Guidelines.

En el formulario de solicitud, el suscriptor deberá identificar y autorizar de forma expresa al Responsable del certificado. Esta autorización deberá ser perfeccionada con una aceptación voluntaria y expresa por parte de la persona física que asume la calificación de Responsable del Certificado.

3.3. Identificación y autenticación para solicitudes de renovación de claves

3.3.1. Identificación y autenticación para la renovación de claves rutinarias

Según lo definido en la DPC de ANF AC.

3.3.2. Identificación y autenticación para renovación de claves tras revocación

Según lo definido en la DPC de ANF AC.

3.4. Identificación y autenticación para solicitudes de revocación

Según lo definido en la DPC de ANF AC.

4. REQUERIMIENTOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

4.1. Solicitud del certificado

4.1.1. Quien puede solicitar un certificado

La solicitud de certificado debe ser realizada por una persona física, mayor de edad, actuando por cuenta propia o como representante legal de un tercero.

En el caso de los Certificados EV y QWAC, ANF AC solo emitirá este tipo de certificados a los Solicitantes que cumplan con los requisitos de Organización Privada, Entidad Gubernamental, Entidad de negocios y Entidad No Comercial especificados en el apartado 8.5 de los EV Guidelines de CA/B Forum.

4.1.2. Proceso de solicitud y responsabilidades

4.1.2.1. Proceso de solicitud de certificados DV y OV

ANF AC obtiene la siguiente documentación del solicitante:

1. Una solicitud de certificado, que puede ser electrónica; y
2. Un contrato de suscripción firmado manuscritamente o meditante firma electrónica.

En el momento que ANF AC reciba la solicitud, comenzará el proceso de verificación.

4.1.2.2. Proceso de solicitud de certificados EV

ANF AC obtiene la siguiente documentación del solicitante:

1. Una solicitud de certificado, que puede ser electrónica; y
2. Un contrato de suscripción firmado.
3. *(Opcional)* Carta de autorización, mediante la cual se autoriza a una o varias personas a desempeñar las funciones descritas en el rol de apobador de certificados. En ese caso, deberá incluir la firma del suscriptor, además de la de las personas autorizadas, que, a partir de ese momento, podrán solicitar/aprobar certificados.

El contrato de suscripción podrá ser enviado:

a) **Presencialmente:** el suscriptor podrá personarse ante una Autoridad de Registro Reconocida, en cuya presencia procederá a firmar el formulario de solicitud, que deberá estar debidamente cumplimentado.
b) **Por correo ordinario:** formulario de solicitud de certificado firmado manuscritamente por el suscriptor y legitimada su firma por Notario Público. Documentación remitida por correo ordinario.
c) **Electronicamente:** Si los formularios correspondientes han sido firmados electrónicamente mediante un certificado cualificado de firma electrónica.

En el formulario constará que el suscriptor asume la responsabilidad de la veracidad de la información reseñada.

4.2. Procesamiento de la solicitud de certificado

4.2.1. Realización de funciones de identificación y autenticación

El RDE comprobará la documentación aportada por el suscriptor, por la Autoridad de Registro (ARR), o por la Oficina de Verificación Presencial (OVP). ANF AC puede reutilizar validaciones anteriores siempre

haya obtenido los datos o el documento de una fuente especificada en el apartado 3.2 o haya completado la validación de los datos no más de 825 días antes de emitir el certificado.

La función, procedimiento y medida de seguridad aplicadas a los ARR y OVP en los tramites que realizan están de acuerdo con el apartado 1.3.2 definido en la DPC de ANF AC.

En el proceso de validación intervendrá, dando soporte, el Departamento Jurídico y el Departamento Técnico que revisará y validará técnicamente el certificado de petición PKCS#10/CRS. ANF AC es responsable de garantizar que la identidad de cada solicitante se verifique de acuerdo con esta PC y la DPC correspondiente antes de la emisión del certificado.

Antes de emitir un certificado SSL/TLS, ANF AC verifica el DNS para comprobar la existencia de CAA Records para cada dNSName en la extensión subjectAltName del certificado que se va a emitir, de acuerdo con el procedimiento establecido en la RFC 6844. ANF AC procesa los tags "*issue*" e "*issuewild*". El issuer domain name para el CAA Record de ANF AC CAA es “anf.es”. Si se emite el certificado, se emitirá dentro del TTL del registro CAA, u 8 horas, lo que sea mayor. ANF AC respetará el indicador crítico y no emitirá un certificado si ANF AC encuentra una propiedad no reconocida con este conjunto de indicadores.

Además, para identificar posibles solicitudes de certificados sospechosas, ANF AC revisa la base de datos interna de todos los certificados revocados y solicitudes de certificados rechazadas anteriormente debido a sospechas de suplantación de identidad (*phishing*) u otro uso fraudulentos.

Antes de utilizar cualquier fuente de datos como fuente de datos fiable, ANF AC evalúa la fuente por su fiabilidad, precisión y resistencia a la alteración o falsificación. ANF AC toma en consideración los aspectos contemplados en el apartado 3.2.2.7 de los Baseline Requirements.

4.2.1.1. Requerimientos de verificación SSL DV

De acuerdo con el apartado 3.2.2.4 de esta Política de Certificación.

4.2.1.2. Requerimientos de verificación SSL OV

La verificación de la identidad , dirección y país del solicitante se realiza de acuerdo con los apartados 3.2.2.1, 3.2.2.2. y 3.2.2.3. de esta PC. La verificación del control del nombre de dominio se realiza de acuerdo con el apartado 3.2.2.4. de esta PC.

4.2.1.3. Requerimientos de verificación SSL EV

4.2.1.3.1. Verificación de la Existencia e Identidad del Solicitante

Los procedimientos de verificación que se definirán en esta sección se pueden evitar en caso de que exista una **Carta Profesional Verificada** y si se cumplen los siguientes supuestos:

Requerimiento de Verificación	Cumplimentado si…
Existencia e identidad del solicitante	La Carta Profesional Verificada incluye una copia de la documentación acreditativa utilizada para establecer la existencia legal del Solicitante, como un certificado de registro, documentación de incorporación, acuerdo de operación, estatuto o ley reglamentaria. ANF AC confirmará el nombre de la organización del solicitante especificado en la Carta profesional verificada con un QIIS o QGIS.
Nombre “comercial”	La Carta Profesional Verificada indica el nombre comercial bajo el cual el Solicitante realiza negocios, la agencia gubernamental con la que está registrado el nombre comercial y que dicha presentación continúa siendo válida.

Existencia Física	La Carta Profesional Verificada indica la dirección del lugar de negocios de la empresa solicitante o matriz / filial y las operaciones comerciales se realizan allí.
Existencia Operacional	El Solicitante tenga una Cuenta de Depósito a Demanda activa actual en una Institución Financiera Regulada.

Verificación de la Existencia e Identidad del solicitante		
Organización Privada	**Aspectos a verificar**	1. **Existencia legal:** *(no designada en los registros por etiquetas como "inactivo", "inválido", "no actual", o equivalente).* 2. **Nombre de la organización.** 3. **Número de registro o CIF.** 4. **Agente u oficina registrada**.
	Metodos de verificación	Una de las siguientes opciones: 1. Consulta online con: ○ Registro Mercantil u otros registros de obligada inscripción ○ Cámara Nacional de Comercio, o ○ Identificador de entidad legal (LEI) 2. Certificación emitida por el Registro Mercantil o su equivalente, LEI o Cámara de Comercio, con un máximo 30 días antes de la solicitud del certificado SSL EV.
Entidad guberna-mental	**Aspectos a verificar**	1. **Existencia legal.** 2. **Nombre de la entidad.** 3. **Número de registro o CIF:** fecha de constitución, registro o formación del solicitante, o el identificador del acto legislativo que creó la Entidad del Gobierno. Si esta información no está disponible, ANF AC ingresará en un lenguaje apropiado una indicación de que el sujeto es una entidad gubernamental.
	Metodos de verificación	Todos los elementos enumerados se verifican directamente con, o se obtienen directamente de, uno de los siguientes: 1. Consulta con el registro oficial. 2. Boletines oficiales nacionales o regionales competentes para la publicación de la creación de la entidad gubernamental. 3. Consulta con la Entidad gubernamental superior que rige en la misma subdivisión política que el Solicitante (por ejemplo, un Secretario de Estado puede verificar la existencia legal de un Departamento de Estado específico).
Entidad de negocios	**Aspectos a verificar**	1. **Existencia legal.** 2. **Nombre de la organización.** *3.* **Número de registro o CIF.** 4. Identidad de la **Persona Principal[2].**

[2] *Persona principal: Individuo principal: un individuo de una Organización privada, Entidad gubernamental o Entidad de negocio que sea propietario, socio, miembro administrador, director o funcionario, según lo identifique su título de empleado, o un empleado, contratista o agente autorizado por tal entidad u organización para llevar a cabo negocios relacionados con la solicitud, emisión y uso de Certificados EV.*

	Metodos de verificación	Una de las siguientes opciones:
		
		1. Consulta online con:
		  ○ Registro Mercantil u otros registros de obligada inscripción
		  ○ Cámara Nacional de Comercio, o
		  ○ Identificador de entidad legal (LEI)
		
		2. Certificación emitida por el Registro Mercantil o su equivalente, LEI o Cámara de Comercio, con un máximo 30 días antes de la solicitud del certificado SSL EV.
		
		La identidad de la Persona Principal, es decir el solicitante persona física con poderes suficientes de representación de la organización, será validada conforme al apartado 3.2.3. de la presente PC, con las siguientes comprobaciones extra:
		
		En la verificación presencial, ya sea ante un empleado de ANF AC o una Autoridad de Registro de ANF AC, la(s) persona(s) principal(es) deben presentar la siguiente documentación además del documento de identidad:
		
		● **Declaración personal:** nombre completo, dirección residencial, fecha de nacimiento y afirmación de que la información contenida en la solicitud del certificado es verdadera y correcta.
		
		● **Un documento financiero**: Tarjeta de crédito principal vigente, tarjeta de débito vigente, declaración de hipoteca de un prestamista reconocible de al menos seis meses de antigüedad o, un extracto bancario de una institución financiera que tenga menos de seis meses.
		
		● **Documento no financiero**: Facturas originales recientes de una empresa de servicios públicos que confirmen el acuerdo para pagar los servicios a una dirección fija, copia de un estado de cuenta para el pago de un contrato de arrendamiento de los últimos seis meses, un certificado de nacimiento o una factura de impuestos de la autoridad local para el año en curso.
		
		ANF AC puede basarse en una validación presencial realizada por una autoridad que ostente fe pública, siempre que ANF AC haya evaluado el procedimiento de validación y concluido que cumple los requisitos de las EV Guidelines (sección 11.11.3.)
		
		El verificador presencial debe:
		
		● Dar fe de la firma de la Declaración Personal y la identidad del firmante; y
		● Identificar los documentos originales de verificación utilizados para realizar la identificación. Además, el Validador de terceros DEBE confirmar en una copia del documento de identificación con foto emitido por el gobierno y firmado que se trata de una reproducción completa, verdadera y precisa del original.

Entidad no comercial *(Org. Interna-cional)*	**Aspectos a verificar**	1. **Existencia legal:** organización internacional legalmente reconocida. 2. **Nombre de la entidad.** 3. **Número de registro o CIF:** fecha de formación o identificador del acto legislativo que creó la Entidad de Organización Internacional. En circunstancias donde esta información no está disponible, ANF AC deberá ingresar el idioma apropiado para indicar que el sujeto es una Entidad de organización internacional.
	Metodos de verificación	Todos los items listados son verificados ya sea: ● Documento constitutivo bajo el cual se formó la Organización Internacional; o ● Directamente en cualquier lista actual de entidades calificadas que CA/Browser Forum mantenga en www.cabforum.org. ● En los casos en que la Organización Internacional sea un órgano, una agencia, o una organización no gubernamental dependiente de una Organización Internacional verificada, ANF AC verificará al Solicitante directamente con la Organización Internacional matriz.

Verificación de DBA/Nombre comercial
ANF AC no permite el uso de un DBA. Tampoco se permite el uso de un nombre comercial.

Verificación de la existencia física del solicitante
Para verificar la existencia física y la presencia comercial del Solicitante, ANF AC verifica que la dirección física provista por el Solicitante es una dirección donde realiza operaciones comerciales (no, por ejemplo, un buzón de correo o un apartado de correos) y es la dirección del lugar de negocios del solicitante. ● Si el domicilio de actividad reseñado en la solicitud aparece reseñado en la fuente oficial consultada para la verificación de la identidad de la organización, no se realizan comprobaciones adicionales. ● Si el domicilio de actividad reseñado en la solicitud no aparece en la fuente oficial, aparece reseñado en al menos una fuente oficial distinta a la utilizada para verificar la existencia legal, ANF AC confirmará que la dirección del domicilio de actividad es una dirección comercial válida por referencia a dicha fuente oficial; ● En el caso de que el domicilio de actividad reseñado en la solicitud no pueda ser validado mediante el procedimiento anterior, ANF AC confirmará la validez de la dirección proporcionada por el solicitante en la solicitud mediante una visita a la dirección comercial realizada por un empleado de ANF AC o un tercero autorizado. Se deberán obtener las evidencias siguientes: a) El negocio del Solicitante se encuentra en la dirección exacta indicada en la Solicitud, b) Identificar el tipo de instalación (por ejemplo, la oficina en un edificio comercial, residencia privada, escaparate, etc.) y si parece ser una ubicación comercial permanente, c) Indicar si hay un signo permanente que identifique al solicitante, d) Indicar si existe evidencia de que el Solicitante está llevando a cabo actividades comerciales continuas en el sitio, y

e) Incluir una o más fotos de (i) el exterior del sitio (con letreros que indiquen el nombre del Solicitante, si está presente, y que muestre la dirección de la calle si es posible), y (ii) el área de recepción interior o el área de trabajo.

- Si lugar de negocios que no se encuentra en el país de constitución o registro: ANF AC se basará en una documento notarial que certifique la dirección del lugar de negocios del solicitante y que las operaciones comerciales se realicen allí.

Verificación de los métodos de comunicación
ANF AC verifica un número de teléfono, número de fax, dirección de correo electrónico para ayudar a comunicarse con el Solicitante y confirmar que el Solicitante conoce y aprueba la emisión. Para verificar un método verificado de comunicación con el solicitante, ANF AC: (A) Mediante: ● registros proporcionados por la compañía telefónica correspondiente; ● una fuente oficial o independiente cualificada; o ● una Carta Profesional Verificada; y (B) Confirmar el método de comunicación obteniendo una respuesta afirmativa del mismo (por ejemplo: llamada telefónica, email con acuse de recibo). En caso de discrepancia entre la documentación proporcionada y la verificación, se verificará que la dirección que figura en la solicitud corresponde a una ubicación en la que la Organización del sujeto opera de manera constante. La dirección de correo electrónico y el servicio de SMS asociado con su teléfono móvil se considerarán como buzones autorizados para que ANF AC pueda entregar correo electrónico certificado, incluida la doble autenticación en el caso de un servicio de firma electrónica centralizada, o cualquier otro que se considere necesario. El usuario asume la obligación de informar a ANF AC de cualquier cambio de dirección de correo electrónico o número de teléfono móvil.

Verificación de la Existencia operacional del solicitante
ANF AC verifica la capacidad comercial mediante la existencia operativa del Solicitante. (1) Si se trata de una entidad gubernamental, ANF AC se basa en la verificación realizada en "Verificación de la existencia e identidad del solicitante" En otros casos, mediante uno de los procesos siguientes: (2) Verificar que el Solicitante ha existido durante al menos tres años, según lo indican los registros de un Registro Oficial; (3) Verificación de que el solicitante figura en un Fuente de Información Independiete Qualificada o en un registro de Hacienda; o (4) Verificación, mediante documentación autenticada, de que el Solicitante dispone de una cuenta bancaria operativa en una Institución Financiera Regulada (certificado bancario);

4.2.1.3.2. Verificación del Nombre de Dominio

Para cada Nombre de dominio completo (FQDN) en un Certificado, ANF AC verificará el control de dominio mediante un procedimiento especificado en el apartado 3.2.2.4 de esta PC.

ANF AC comparará visualmente cualquier nombre de dominio con caracteres mixtos con dominios de alto riesgo conocidos. Si se encuentra una similitud, entonces la solicitud de certificado EV debe marcarse como de alto riesgo. En ese caso, ANF AC realizará procesos de autenticación y verificación adicionales para asegurarse, ante toda duda razonable, de que el Solicitante y el objetivo en cuestión son la misma organización

4.2.1.3.3. Verificación de autorización del solicitante para el Certificado EV

Verificación del nombre, cargo y autoridad de: Firmante del contrato y del Aprobador de certificados	
Nombre y cargo	• DNI • Escritura de poder y/o Registro oficial Se verifica que el suscriptor no está registrado en la lista negra de individuos y entidades con OID 1.3.6.1.4.1.18332.56.3.1, o está operando en un lugar donde las políticas de CA prohíben la emisión de certificados (documento con OID 1.3.6.1). 4.1.18332.56.2.1). ANF AC actualiza regularmente su base de datos con todas las personas que aparecen en la búsqueda e incautación, y enlaza esta lista negra con el control de solicitud de certificado.
Facultad del firmante del contrato	En caso de que la figura del firmante no coincida con el solicitante del certificado, se incluirá: • Una declaración jurada, donde se reconoce que el firmante está autorizado para actuar en nombre del solicitante para solicitar un Certificado SSL EV a ANF AC, y para usar y asegurar el certificado emitido. De este modo, se verifica la facultad del firmante del contrato del suscriptor; o • Clausula añadida en el contrato de suscripción con el contenido establecido en el Apéndice E de los EV Guidelines.
Facultad EV de Aprobador de Certificados	En el caso de que la figura del aprobador de Certificados no coincida con el solicitante del certificado deberá existir una carta de autorización, reseñada en el apartado 4.1.2.2. de la presente PC. La carta deberá incluir las firmas de cada una de las personas autorizadas, además de la firma del firmante del contrato.

Verificación de la firma en el acuerdo del suscriptor y las solicitudes de certificado EV
Tanto el Acuerdo de Suscriptor como cada Solicitud de Certificado EV deben estar firmadas. El método para autenticar la firma del Solicitante de Certificado o el Firmante del Contrato será uno de los siguientes: 1. Presencia física del suscriptor ante un Operador de ANF AC, empleado o tercero autorizado, quien también firma acreditando la verificación. 2. Legitimación notarial de la firma(s) insertada(s) en el contrato.

Verificación de aprobación de solicitud de certificado EV
En caso de que la figura del aprobador de certificados sea distinta del solicitante, para verificar la aprobación del Aprobador de Certificados de una Solicitud de Certificado EV, ANF AC se pondrá en contacto con el Aprobador de certificados utilizando un método de comunicación verificado para el solicitante y obtener una confirmación oral o por escrito de que el Aprobador de certificados ha revisado y aprobado la Solicitud de certificado EV.

ANF AC verifica si el Solicitante, el Firmante del Contrato, el Aprobador del Certificado, la Jurisdicción de Incorporación, Registro o domicilio de actividad del Solicitante está identificado en cualquier lista denegada por el gobierno, lista de personas prohibidas OID 1.3.6.1.4.1.18332.56.3.1, u otra lista que prohíba hacer negocios con dicha organización o persona según las leyes del país de la (s) jurisdicción (es) de la CA; o tiene su Jurisdicción de Incorporación, Registro o Lugar de Negocio en cualquier país con el cual las leyes de la jurisdicción de la CA prohíban hacer negocios (documento con OID 1.3.6.1.4.1.18332.56.2.1). ANF AC no emitirá ningún Certificado EV al Solicitante si el Solicitante, el Firmante del Contrato o el Aprobador de Certificados o si la Jurisdicción de Incorporación o Registro del Solicitante o el Lugar de Negocios se encuentran en dicha lista.

ANF AC actualiza regularmente su base de datos con todas las personas que aparecen en la búsqueda e incautación, y vincula esta lista negra al control de solicitud de certificado.

4.2.1.4. Requerimientos de verificación QWAC

Todos los requisitos de verificación definidos en la sección 4.2.1.4. de esta PC se aplican al Certificado QWAC expedido a personas jurídicas. Para los QWAC emitidos a personas físicas, se deben seguir los procedimientos establecidos en los Baseline Requirements de CA/B Forum.

Además, en los Certificados EV SSL de PSD2, ANF AC verificará, usando información auténtica de la Autoridad Nacional Competente, los atributos específicos de PSD2:

- numero de autorización,
- roles PSP, y
- Nombre de la Autoridad Nacional Competente proporcionada por el sujeto.

Si la Autoridad Nacional Competente proporciona estándares para la validación de estos atributos, ANF AC aplicará esos estándares.

4.2.1.5. Requerimientos de verificación Sede Electronica

La verificación de la identidad del solicitante se realiza de acuerdo con los apartados 3.2.2.1. y 3.2.2.2. de esta PC. Si el campo subject:countryName está presente, el país se verifica de acuerdo con el apartado 3.2.2.3. de esta PC. La verificación del control del nombre de dominio se realiza de acuerdo con el apartado 3.2.2.4. de esta PC.

- Comprobación de pertenencia del número de teléfono fijo (no móvil) a la entidad sujeto en:
- Páginas de operadores telefónicos, Agencias de Protección de Datos.
- Mediante llamada directa

Para la designación de sedes electrónicas dentro de una organización, se seguirán criterios claros y sin ambigüedad de la sede. No se prescribe un número o criterio concreto para determinar el número de sedes existentes en un organismo público o departamento ministerial.

Ejemplos de designación de sedes electrónicas serían (“Nombre descriptivo de la sede electrónica”):

- "Centro de Transferencia de Tecnologías de las Administraciones Públicas"
- "Punto de Acceso General
- "Portal oficial del Ministerio de la Presidencia"

Comprobación de la existencia operativa. Las entidades privadas deberán acreditar que realizan movimientos bancarios con una institución financiera regulada.

ANF AC realiza una comprobación dual, interviniendo el Área Técnica y la Asesoría Jurídica. Además, en los mismos casos todas las validaciones son revisadas por el Responsable del Área Técnica.

Si el certificado tiene el carácter de Validación Extendida (EV), se seguirán los procedimientos de verificación especificados en la sección 4.2.1.4.

4.2.1.6. Estado de Alto Riesgo

Se consideran solicitudes de certificados de alto riesgo aquellas ANF AC marca para escrutinio adicional por referencia a criterios internos y bases de datos mantenidas por ANF AC, que pueden incluir:

- Nombres con mayor riesgo de phishing u otro uso fraudulento,
- Nombres contenidos en solicitudes de certificados previamente rechazadas o certificados revocados,
- Los nombres que figuran en la lista de phishing de Miller Smiles o en la lista de navegación segura de Google, o
- Nombres que ANF AC identifica utilizando sus propios criterios de mitigación de riesgos.

A ANF AC mantiene procedimientos documentados que identifican y requieren verificaciones adicional para las Solicitudes de Certificados de Alto Riesgo antes de la validación del certificado, según sea razonablemente necesario para garantizar que dichas solicitudes se verifiquen correctamente.

4.2.2. Aprobación o rechazo de solicitudes

El Responsable de Dictámenes de Emisión (RDE) asume la responsabilidad última de verificar la información contenida en el Formulario de Solicitud, valorar la suficiencia de los documentos aportados y la adecuación de la solicitud, de acuerdo con lo establecido en el apartado 4.2.1. de esta PC.

ANF AC rechazará cualquier solicitud de certificado que no pueda ser verificada.

Además, el RDE determinará:

- Que el suscriptor ha tenido acceso a la información que establece los términos y condiciones relativos al uso del certificado, así como a las tasas de emisión del mismo.
- Que el suscriptor ha tenido acceso y tiene permanente acceso a toda la documentación relativa a las obligaciones y responsabilidades de la CA, del suscriptor, sujeto, responsable del certificado y terceros que confían, en especial a la DPC y a las Políticas de Certificación.

También supervisará que se cumplen todos los requisitos impuestos por la legislación aplicable en materia de protección de datos, siguiendo lo establecido en el documento de seguridad incluido en la DPC.

El proceso de emisión del certificado no se iniciará en tanto en cuanto el Responsable de Dictámenes de Emisión no haya emitido el correspondiente informe de conformidad. El plazo máximo establecido para la emisión del informe será de 15 días. Transcurrido ese plazo sin emisión del preceptivo informe, el suscriptor podrá dar por anulado el pedido y recibir las tasas que haya abonado.

El RDE puede requerir del suscriptor información o documentación complementaria y el suscriptor dispondrá de 15 días para hacer entrega de la misma. Transcurrido este plazo sin que se haya

cumplimentado este requerimiento, el RDE emitirá informe denegando la emisión. En caso de atender el requerimiento, el RDE dispondrá de 7 días para emitir informe definitivo.

En caso de que el RDE compruebe que la información facilitada por el suscriptor no es veraz, denegará la emisión del certificado, generará un incidente informando al Coordinador de Seguridad, a fin de determinar la inclusión o no del suscriptor en la lista negra de personas y entidades 1.3.6.1.4.1.18332.56.2.1.

ANF AC comprueba por si misma, o por medio de sus Autoridades de Registros, u Oficinas de Verificación Presencial, la solicitud, la identidad, la dirección y cualesquiera otras circunstancias de los suscriptores y sujetos de los certificados. El instrumento legal existente entre las partes incluirá la exigencia de cumplimiento de lo indicado en los requisitos de ETSI y CA/B Forum.

4.2.3. Tiempo para procesar las solicitudes de certificado

Según lo definido en la DPC de ANF AC.

4.3. Emisión de certificados

La emisión del certificado es como se define en la DPC de ANF AC. ANF AC evitará generar certificados que caduquen en fecha posterior a la caducidad de certificados de CA emsiora.

4.3.1. Actuaciones de la CA durante la emisión del certificado

Según lo definido en la DPC de ANF AC.

Previo a la emisión del certificado, el sistema de emisión procede a la validación del formato del certificado mediante herramienta de linting Zlint, x509lint y certlint.

4.3.2. Notificación al suscriptor por parte de la CA de la emisión del certificado

Según lo definido en la DPC de ANF AC.

4.4. Aceptación del certificado

4.4.1. Conducta constitutiva de aceptación del certificado

Según lo definido en la DPC de ANF AC.

4.4.2. Publicación del certificado por la CA

Según lo definido en la DPC de ANF AC.

4.4.3. Notificación de la emisión del certificado a otras entidades

Solo en el caso de los certificados PSD2, si se notificó a ANF AC la dirección de correo electrónico de la Autoridad Nacional Competente (NCA) identificada en la emisión del nuevo certificado, ANF AC enviará a esta dirección de correo electrónico la información del contenido del certificado, así como información de contacto e instrucciones para solicitudes de revocación.

4.5. Par de claves y uso del certificado

4.5.1. Uso del certificado y clave privada por el suscriptor

Ver apartado 9.6.3, provisiones 2. y 4.

4.5.2. Uso del certificado y clave pública por terceros que confían

Según lo definido en la DPC de ANF AC.

4.6. Renovación del certificado sin cambio de claves

4.6.1. Circunstancias para la renovación del certificado

Según lo definido en la DPC de ANF AC.

4.6.2. Quien puede solicitar la renovación

Según lo definido en la DPC de ANF AC.

4.6.3. Procesamiento de solicitudes de renovación

El proceso para remisión/renovación es el mismo que para nueva emisión. La documentación que debe aportar el suscriptor y los pasos de validación, emisión y entrega de certificados son los mismos que para la emisión de un certificado nuevo.

Se contemplan dos modalidades de renovación:

- Renovación de certificados con cambio de clave
- Renovación de certificados sin cambio de clave

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento. Antes de la renovación de los certificados PSD2, ANF AC repetirá la verificación de los atributos específicos de PSD2 incluidos en el certificado. Si la Autoridad Nacional Competente proporciona normas para la validación de estos atributos, ANF AC aplicará esas normas.

4.6.4. Notificación de nueva emisión de certificado al suscriptor

Según lo definido en la DPC de ANF AC.

4.6.5. Conducta constitutiva de aceptación de la renovación

Según lo definido en la DPC de ANF AC.

4.6.6. Publicación del certificado renovado por la CA

Según lo definido en la DPC de ANF AC.

4.6.7. Notificación de la emisión del certificado a otras entidades

Ninguna estipulación. No se notifica a terceros.

4.7. Renovación del certificado con cambio de claves (Re-key)

Según lo definido en la DPC de ANF AC.

4.8. Modificación del certificado

No aplicable.

4.9. Renovación y suspensión del certificado

Con caracter general, según lo definido en la DPC de ANF AC.

4.9.1. Circunstancias para la revocación

ANF AC deberá revocar un certificado en un período de 24 horas si se da una más de las siguientes circunstancias:

1. El Suscriptor solicita por escrito que ANF AC revoque el Certificado;

2. El Suscriptor notifica a ANF AC que la solicitud de certificado original no fue autorizada y no otorga retroactivamente la autorización;
3. ANF AC obtiene evidencia de que la Clave Privada del Suscriptor correspondiente a la Clave Pública en el Certificado sufrió un Compromiso de la Clave;
4. ANF AC obtiene evidencia de un método demostrado o comprobado que puede calcular fácilmente la clave privada del suscriptor basándose en la clave pública en el certificado (como una Debian weak key, consulte https://wiki.debian.org/SSLkeys);
5. ANF AC obtiene evidencia de que no se debe confiar en la validación de la autorización o el control del dominio para cualquier Nombre de Dominio (FQDN) o Dirección IP en el Certificado.

ANF AC deberá revocar un certificado en un período de 5 días si se da una o más de las siguientes circunstancias:

1. El Certificado ya no cumple con los requisitos de los apartados 6.1.5 y 6.1.6 de los CA/B Forum Baseline Requirements;
2. ANF AC obtiene evidencia de que el certificado fue utilizado de forma incorrecta;
3. ANF AC tiene conocimiento de que un Suscriptor ha violado una o más de sus obligaciones importantes en virtud del Contrato de Suscripción o los Términos y Condiciones;
4. ANF AC tiene conocimiento de cualquier circunstancia que indique que el uso de un Nombre de dominio (FQDN) o una Dirección IP en el Certificado ya no está legalmente permitido (por ejemplo: un tribunal ha revocado el derecho de un Registrador de Nombre de Dominio a usar el Nombre de Dominio, la licencia o el acuerdo de servicios entre el Registrador de Nombre de Dominio y el Solicitante ha finalizado, o el Registrador de Nombre de Dominio no ha renovado el Nombre de Dominio);
5. ANF AC tiene conocimiento de que se ha utilizado un certificado Wildcard para autenticar un nombre de dominio engañoso o fraudulento;
6. ANF AC tiene conocimiento de un cambio importante en la información contenida en el Certificado;
7. ANF AC tiene conocimiento de que el Certificado no se emitió de acuerdo con los Baseline Requirements de CA/B Forum, esta Política de Certificación o la Declaración de práctica de certificación de ANF AC;
8. ANF AC determina o se le informa que cualquiera de la información que aparece en el Certificado es inexacta;
9. El derecho de ANF AC a emitir Certificados conforme a los Baseline Requirements de CA/B Forum expira o se revoca o finaliza, a menos que ANF AC haya hecho arreglos para continuar manteniendo el Repositorio de CRL / OCSP;
10. La revocación es requerida por la Política de Certificación de ANF AC y / o la Declaración de Práctica de Certificación; o
11. ANF AC tiene conocimiento de un método demostrado o comprobado que expone la Clave privada del suscriptor a un compromiso o si existe evidencia clara de que el método específico utilizado para generar la clave privada fue defectuoso.

ANF AC deberá revocar un certificado de CA intermedia en un período de siete (7) días si ocurre una o más de las siguientes circunstancias:

1. La CA intermedia solicita la revocación por escrito;
2. La CA intermedia notifica a ANF AC que la solicitud de certificado original no fue autorizada y no otorga retroactivamente la autorización;
3. ANF AC obtiene evidencia de que la Clave Privada de la CA intermedia correspondiente a la Clave Pública en el Certificado sufrió un Compromiso de la Clave o ya no cumple con los requisitos de los apartados 6.1.5 y 6.1.6 de los Baseline Requirements de CA/B Forum;
4. ANF AC obtiene evidencia de que el certificado fue mal utilizado;

5. ANF AC tiene conocimiento de que el Certificado no se emitió de conformidad con o que la CA intermedia no ha cumplido con este documento o con Declaración de Prácticas de Certificación de ANF AC;
6. ANF AC determina que cualquiera de la información que aparece en el certificado es inexacta;
7. ANF AC o la CA intermedia deja de operar por cualquier motivo y no ha hecho arreglos para que otra CA brinde soporte de revocación para el certificado;
8. El derecho de ANF AC o CA intermedia a emitir Certificados conforme a los requisitos de CA/B Forum ha caducado, ha sido revocado o ha finalizado, a menos que la ANF AC haya hecho arreglos para continuar manteniendo el Repositorio de CRL / OCSP; o
9. La revocación es requerida por la Política de Certificación de ANF AC y / o la Declaración de Prácticas de Certificación.

En los certificados PSD2, si la Autoridad Nacional Competente, como propietaria de la información específica de PSD2, notifica a ANF AC que ha cambiado la información relevante, ANF AC investigará esta notificación, independientemente de su contenido y formato. ANF AC determinará si los cambios afectan la validez del certificado, en cuyo caso revocará el(los) certificado(s) afectado(s). ANF AC llevará a cabo esta verificación y evaluación en un plazo máximo de 72 horas, a menos que la demora esté justificada.

ANF AC procesará estas solicitudes y validará su autenticidad. Si no se proporciona una razón o la razón no está en el área de responsabilidad de la Autoridad Nacional Competente, ANF AC puede decidir no tomar medidas. Basándose en una solicitud auténtica, ANF AC revocará el certificado si se cumple alguna de las siguientes condiciones:

- La autorización de PSP ha sido revocada,
- el número de autorización de la PSP ha cambiado,
- el nombre o identificador de la Autoridad Nacional Competente ha cambiado,
- se ha revocado cualquier rol de PSP incluido en el certificado,
- La revocación es obligatoria por ley.
- Cualquier otra causa de revocación establecida en esta Política de Certificación.

4.9.2. Quien puede solicitar una revocación

Según lo establecido en la DPC de ANF AC. Además, los suscriptores, los terceros que confían, los proveedores de software de aplicación, las autoridades nacionales competentes y otros terceros pueden presentar informes de problemas de certificados para comunicar a ANF AC una circunstancia razonable para revocar el certificado.

4.9.3. Procedimiento de solicitud de revocación

Según lo establecido en la DPC de ANF AC.

ANF AC facilita instrucciones y da soporte jurídico para la presentación de denuncias o sospechas de compromiso de la clave privada, de mal uso de certificados o cualquier tipo de fraude o por conducta impropia.

Puede interponer directamente su sospecha o denuncia en: https://www.anf.es/sat-incumplimiento-uso-indebido/

ANF AC dispone de un servicio 24x7 para responder solicitudes de revocaciones o incidentes relacionados con los certificados. Cualquier persona que necesite instrucciones tecnicas o soporte legal en este area, puede realizar sus consultas de maner gratuita mediante cualquiera de los siguientes procedimientos:

- En horario laboral, al teléfono 902 902 172 (Llamadas desde España), Internacional +34 933 935 946, o mediante personación en sus dependencias.

- Fuera del horario de oficina, mediante llama al teléfono +34 930 502 397
- Online. Rellenando el formulario publicado en web: https://www.anf.es/
- Servicio online. https://www.anf.es/ac/revocar-certificado-web
- Enviando un correo a: soporte@anf.es

Las Autoridades Nacionales Competentes, para notificar cambios en la información PSD2 relevante de un Proveedor de Servicios de Pago (PSP), pueden enviar un correo electrónico a info@anf.es

- ANF AC investigará las incidencias de las que tenga conocimiento dentro de las veinticuatro horas siguientes a su recepción. El Responsable de Seguridad, en base a las indagaciones y comprobaciones realizadas, emitirá informe al Responsable de Dictámenes de Emisión, el cual determinará, en su caso, la correspondiente revocación mediante Acta fundamentada, en la cual constará:
  - Naturaleza de la incidencia.
  - Informaciones recibidas.
  - Normas legales y regulación sobre la que se fundamente la orden de revocación.
- Cualquier persona interesada puede abrir una incidencia mediante alguno de los siguientes procedimientos:
  - Mediante llamada telefónica en horario de oficina: 902 902 172 (llamadas desde España) (lunes a viernes de 9 h. a 18 h.) +34 933 935 946 (Internacional)
  - Procedimiento online. El interesado debe abrir una incidencia en el servicio web: https://www.anf.es/ac/abrir-incidencia

4.9.4. Periodo de gracia de solicitud de revocación

Según lo definido en la DPC de ANF AC.

4.9.5. Plazo máximo de procesamiento de la solicitud de revocación

Dentro de las 24 horas posteriores a la recepción de un Informe de problemas con el certificado, ANF AC investigará los hechos y circunstancias relacionados con la solicitud de revocación y proporcionará un informe preliminar sobre sus hallazgos tanto al Suscriptor que solicita la revocación como a la entidad que contactó con ANF AC par notificar un problema con el certificado. .

ANF AC, después de revisar los hechos y circunstancias, trabajará con el suscriptor y cualquier entidad que informe el problema de certificado u otro aviso relacionado con la revocación para establecer si el certificado será revocado o no, y en su caso, la fecha en la que ANF AC revocará el certificado. El período desde la recepción del Informe de Problema del Certificado o la notificación relacionada con la revocación hasta la revocación publicada no deberá exceder el período de tiempo establecido en la Sección 4.9.1.1.

ANF AC cuenta con un Registro de incidentes en el que se registran todos los incidentes ocurridos con los certificados emitidos y las evidencias obtenidas. Estos incidentes se registran, analizan y resuelven de acuerdo con los procedimientos del Sistema de Gestión de Seguridad de la Información de ANF AC.

El Responsable de seguridad determina la gravedad del incidente y nombra a un responsable y, en caso de incidentes de seguridad significativos, informa a la Junta Rectora de la PKI. En casos de fraude o *phishing*, la información se reporta al sitio del Anti-Phishing Working Group,

https://apwg.org/

4.9.6. Requerimientos de verificación de revocación de terceros que confían

Según lo establecido en la CPC de ANF CA.

4.9.7. Frecuencia de emisión de CRL y ARL

Según lo establecido en la CPC de ANF CA.

4.9.8. Periodo máximo de publicación de CRL y ARL

Según lo establecido en la CPC de ANF CA.

4.9.9. Disponibilidad de servicio de verificación de estado de certificado

ANF AC pone a disposición de los terceros que confían un servicio de verificación de revocación en línea, que está disponible las 24 horas del día, los 7 días de la semana.

4.9.10. Requisitos de verificación de estado de certificado

Los terceros que confían pueden verificar en línea la revocación de un certificado en el sitio web https://www.anf.es/en

El sistema de consulta de certificados de ANF AC requiere el conocimiento previo de algunos parámetros del certificado de interés. Este procedimiento evita la recolección masiva de datos.

Este servicio cumple con los requisitos en términos de protección de datos personales y solo proporciona copias de estos certificados a terceros debidamente autorizados.

El acceso a este sistema es gratuito.

4.9.11. Otras formas de información de revocación de certificados disponibles

Ninguna estipulación.

4.9.12. Requisitos especiales en cuanto a compromiso de la clave privada

Ver apartado 4.9.1.

4.9.13. Circunstancias para la suspensión

No aplicable. No se permite la suspensión.

4.10. Servicios para la comprobación de estado del certificado

Según lo establecido en la DPC de ANF AC.

4.11. Fin de suscripción

Según lo establecido en la DPC de ANF AC.

4.12. Custodia y recuperación de claves

Según lo establecido en la DPC de ANF AC.

A excepción de los certificados centralizados de firma electrónica, ANF AC no almacena, ni tiene la capacidad de almacenar la clave privada de los suscriptores y, por lo tanto, no proporciona el servicio de recuperación de claves.

5. INSTALACIÓN, GESTIÓN Y CONTROLES OPERATIVOS

5.1. Controles físicos

Según lo establecido en la DPC de ANF AC.

5.2. Controles de procedimiento

Según lo establecido en la DPC de ANF AC.

5.3. Controles de personal

Según lo establecido en la DPC de ANF AC.

5.4. Procedimientos de registro de auditoría

Según lo establecido en la DPC de ANF AC.

5.5. Archivo

Según lo establecido en la DPC de ANF AC.

5.6. Cambio de claves de CA (Key changeover)

Según lo establecido en la DPC de ANF AC.

5.7. Compromiso y recuperación ante desastres

Según lo establecido en la DPC de ANF AC.

5.8. Cese de CA o AR

Según lo establecido en la DPC de ANF AC.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación del par de claves

Según lo establecido en la DPC de ANF AC.

6.1.2. Entrega de la Clave Privada al suscriptor

Como se establece en la DPC de ANF AC, ANF AC entrega a sus usuarios los dispositivos/software criptográficos necesarios para generar en privado y sin intervención de terceros, su par de claves y los datos de activación de las mismas. Esto asegura el cumplimiento de los parámetros establecidos en los BR apartado 6.1.5 y 6.1.6. Es el propio suscriptor quien se genera y está en posesión de la clave privada.

ANF AC no genera las claves de los certificados de entidad final que tienen una extensión EKU que contiene KeyPurposeIds id-kp-serverAuth o anyExtendedKeyUsage.

En el caso de ANF AC o cualquiera de sus AR designadas tuvieran conocimiento de que la clave privada del suscriptor hubiera sido comunicada a una persona no autorizada o una organización no afiliada con el suscriptor, ANF AC procedería a la revocación todos los certificados que incluyeran la clave pública correspondiente a la clave privada comunicada.

6.2. Controles de protección de claves privadas y módulos criptográficos de ingeniería

Según lo establecido en la DPC de ANF AC.

6.3. Otros aspectos de la gestión del par de claves

Según lo establecido en la DPC de ANF AC.

6.4. Datos de activación

Según lo establecido en la DPC de ANF AC.

6.5. Controles de seguridad informática

Según lo establecido en la DPC de ANF AC.

6.6. Controles técnicos del ciclo de vida

Según lo establecido en la DPC de ANF AC.

6.7. Controles de seguridad de red

Según lo establecido en la DPC de ANF AC.

6.8. Time-stamping

Según lo establecido en la DPC de ANF AC.

7. PERFILES DE CERTIFICADO, CRL Y OCSP

El certificado incorpora información estructurada conforme con el estándar X.509 v3 de la IETF, tal y como se especifica en la especificación RFC 5280 *(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).*

7.1. Perfil de certificado

7.1.2. Numero(s) de versión

x.509 v3.

7.1.3. Contenido y Extensiones de Certificado; Aplicacion de RFC 5280

ANF AC utiliza extensiones de certificado de acuerdo con los estándares de la industria aplicables, incluido RFC 3280/5280.

Los certificados de CA intermedia tecnicamente restringida *(Technically Constrained Subordinate CA)* deben incluir una extensión de Uso de clave extendida (EKU) que especifique todos los usos de claves extendidos para los cuales el certificado de CA intermedia está autorizado para emitir certificados. AnyExtendedKeyUsage KeyPurposeId no aparecerá en la extensión EKU de certificados de confianza pública.

El período de validez del certificado se describe en Tiempo Universal Coordinado y se codifica según la especificación RFC 5280.

La clave pública del sujeto está codificada según la especificación RFC 5280, así como la generación y codificación de la firma.

Dentro de los certificados, además de los campos comunes ya estandarizados, también se incluye un grupo de campos "propietarios" que proporcionan información en relación con el suscriptor u otra información de interés.

Extensión	Critical	Value
basicConstraints	-	Optional. cA field is not set true
keyUsage	-	Optional. Bit positions for keyCertSign and cRLSign are NOT set.
certificatePolicies	NO	certificatePolicies:policyIdentifier A Policy identifier, defined by ANF AC that indicates a Certificate Policy asserting ANF AC's adherence to and compliance with the applicable requirements.
extendedKeyUsage	NO	id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. Other values are NOT present.
cRLDistributionPoints	NO	HTTP URL of ANF AC's CRL service
authorityInformationAccess	NO	HTTP URL of the issuing CA's OCPS responder (accessMethod=1.3.6.1.5.5.7.48.1)
authorityKeyIdentifier	NO	keyIdentifier field and it MUST NOT contain a authorityCertIssuer or authorityCertSerialNumber field.

ANF AC no emitirá un certificado que contenga una keyUsage flag, ExtendedKeyUsage value, extensión de certificado u otros datos no especificados anteriormente, a menos que tenga conocimiento de una razón para incluir esos datos en el certificado.

No se incluirán extensiones que no apliquen en el contexto de Internet público (como un valor extendedKeyUsage para un servicio que solo es válido en el contexto de una red administrada de forma privada), a menos que:

i. dicho valor caiga dentro de un OID para el cual el solicitante demuestra la propiedad, o
ii. de lo contrario, el solicitante puede demostrar el derecho de hacer valer los datos en un contexto público;

No se incluirá semántica que induzca a error a los terceros que confían sobre la información del certificado verificada por ANF AC (como incluir el valor de ExtendedKeyUsage para una SmartCard, si ANF AC no puede verificar que la clave privada correspondiente esté limitada a tal hardware debido a una emisión en remoto).

7.1.3.1. Campos propietarios

Se han asignado identificadores unívocos a nivel internacional. Concretamente:

- Los campos referenciados con el identificador de objeto (OID) 1.3.6.1.4.1.18332.x.x, son extensiones propietarias de ANF AC. La relación completa de códigos OID y la información asociada a los mismos puede ser consultada en la Sección "Campos Propietarios ANF AC" de la Declaración de Prácticas de Certificación de ANF AC.
- Los campos con el ISO/IANA del MPR 2.16.724.1.3.5.x.x, son extensiones propietarias requeridas e identificadas en el Esquema de Identificación y Firma Electrónica v.1.7.6 publicado por el Consejo Superior de Administración Electrónica.
- Los campos con el OID 1.3.6.1.4.1.18838.1.1, son extensiones propietarias de la Agencia Estatal de Administración Tributaria (AEAT) Internationally unambiguous identifiers have been assigned. Specifically:

7.1.3.2. QcStatements

Los certificados emitidos por ANF AC siguen lo definido en la ETSI EN 319 412-5 (Certificate ProfilesQCStatements):

- **QcCompliance,** se refiere a una declaración del emisor en la cual se hace constar la calificación con la que es emitido el certificado, y marco legal al que se somete. Concretamente los certificados sometidos a esta política, emitidos con la calificación de reconocidos (cualificados), reseñan: "Este certificado se expide con la calificación de cualificado de acuerdo con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo"

- **QcLimitValue**, informa del límite monetario que asume la CA como responsabilidad en la pérdida de transacciones a ella imputables. Este OID contiene la secuencia de valores: moneda (codificado conforme a la ISO 4217), cantidad y exponente. P.ej. EUROS 100x10 elevado a 1, lo que presupone límite monetario de 1000 EUROS.

  Además, con el fin de facilitar la consulta de esta información, el límite de responsabilidad se incluye en la extensión propietaria del OID 1.3.6.1.4.1.18332.41.1, que reseña el importe expresado en euros. En caso de duda o discrepancia siempre se debe dar preferencia a la lectura del valor reseñado en el OID 1.3.6.1.4.1.18332.41.1

- **QcEuRetentionPeriod**, determina el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este. En el caso de ANF AC, es de 15 años.

- **QcSSCD**, determina que la clave privada asociada a la clave pública contenida en el certificado electrónico, está en un dispositivo cualificado de creación de firma en conformidad con el Anexo II del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

- **QcType**, cuando el certificado se emite con el perfil (FIRMA), se reseña QcType 2

- **QcPDS**, se proporciona la URL en inglés que permite acceder a todas las políticas de la PKI de ANF AC (PDS Policy Disclosure Statements)

- **PSD2QcType**
  Los certificados emitidos por ANF AC del tipo PSD2 además de los campos anteriormente reseñados, se incluye PSD2QcType, conforme lo establecido en la ETSI TS 119 495 clausula 5.1:
  a) La función del Prestador de Servicios de Pago (PSP), que puede ser una o más de las siguientes:
     iii. servicio de cuentas (PSP_AS);
     iv. iniciación de pago (PSP_PI);
     v. información de la cuenta (PSP_AI);
     vi. emisión de instrumentos de pago basados en tarjeta (PSP_IC).
  b) Nombre de la Autoridad Nacional Competente donde el PSP está registrado. Esta información se proporciona en dos formas: la cadena de nombre completo (NCAName) en inglés y un identificador único abreviado (NCAId).

7.1.4. Identificadores de Objeto de los algoritmos utilizados

Según lo establecido en la DPC de ANF AC.

7.1.5. Formatos de nombres

Los atributos del sujeto NO DEBEN contener únicamente metadatos, como los caracteres '.', '-' y '' (espacio), y / o cualquier otra indicación de que el valor está ausente, incompleto o no es aplicable. No se incluye el campo Common Name.

La información sobre el sujeto de los certificados de suscriptor sigue los requisitos especificados en el apartado 7.1.4.2 de los Baseline Requirements.

Los Certificados EV incluirán la información sobre la organización del Sujeto en los campos enumerados en el apartado 9.2 de los EV Guidelines.

7.1.5.1. Extensión Subject Alternative Name

Esta extensión contiene al menos una entrada de un dNSName que contiene un Full Qualified Domain Name. Se permiten los FQDN Wildcard.

Las entradas en dNSName se introducen en la "*preferred name syntax*", como se especifica en RFC 5280. No se aceptan los caracteres "_" en los dNSName.

7.1.6. Restricciones de nombres

Para que un certificado de CA intermedia se considere técnicamente restringido (Technically Constrained), el certificado debe incluir una extensión de uso de clave extendida (EKU) que especifique todos los usos de clave extendida para los cuales el certificado de CA subordinada está autorizado para emitir certificados. AnyExtendedKeyUsage KeyPurposeId NO debe aparecer dentro de esta extensión.

7.1.7. Identificador de objeto (OID) de política de certificado

Cuando ANF AC emite un certificado que contiene uno de los identificadores de política establecidos en el apartado 1.2, afirma que el Certificado se administra de acuerdo con la política que se identifica en este documento.

7.1.8. Uso de la extensión "Policy Constraints"

Según lo definido en la DPC de ANF AC.

7.1.9. Sintaxis y semántica de los calificadores de política

Según lo definido en la DPC de ANF AC.

7.1.10. Tratamiento semántico para la extensión crítica "Certificate Policy"

Según lo definido en la DPC de ANF AC.

7.2. Perfil de CRL

Según lo definido en la DPC de ANF AC.

7.3. Perfil de OCSP

Según lo definido en la DPC de ANF AC.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1. Frecuencia o circunstancias de las auditorías

Según lo definido en la DPC de ANF AC.

8.2. Identidad/Acrediatciones del auditor

Según lo definido en la DPC de ANF AC.

8.3. Relación del auditor con la entidad auditada

Según lo definido en la DPC de ANF AC.

8.4. Aspectos cubiertos por la auditoría

Según lo definido en la DPC de ANF AC.

8.5. Acciones tomadas como resultado de las deficiencias

Según lo definido en la DPC de ANF AC.

8.6. Comunicación de resultados

Según lo definido en la DPC de ANF AC.

8.7. Auditorías internas

Según lo definido en la DPC de ANF AC.

9. ASUNTOS LEGALES Y OTROS

9.1. Tarifas
Según lo definido en la DPC de ANF AC.

9.2. Responsabilidad financiera
Según lo definido en la DPC de ANF AC.

9.3. Confidencialidad de la información
Según lo definido en la DPC de ANF AC.

9.4. Privacidad de la información personal
Según lo definido en la DPC de ANF AC.

9.5. Derechos de propiedad intelectual
Según lo definido en la DPC de ANF AC.

9.6. Obligaciones
Cuando ANF AC emite un certificado EV, ANF AC garantiza a los Beneficiarios del Certificado enumerados en la Sección 9.6.1 durante el período en que el certificado EV es válido que ANF AC ha cumplido con los requisitos de CA/B Forum EV Guidelines, con su DPC y esta PC, en la emisión y administración del certificado EV y en la verificación de la precisión de la información contenida en el certificado EV. Las garantías de certificación EV incluyen las especificadas en la sección 7.1. de los EV Guidelines.

Los suscriptores de certificados EV realizan los compromisos y garantías establecidos en la Sección 9.6.3 de la DPC de ANF AC para el beneficio de la CA y los Beneficiarios del Certificado.

9.7. Exención de garantías
Según lo definido en la DPC de ANF AC.

9.8. Limitaciones de responsabilidad
Según lo definido en la DPC de ANF AC.

9.9. Responsabilidad Civil
Según lo definido en la DPC de ANF AC.

9.10. Periodo de validez
Según lo definido en la DPC de ANF AC.

9.11. Avisos individuales y comunicaciones con los participantes
Según lo definido en la DPC de ANF AC.

9.12. Enmiendas
Según lo definido en la DPC de ANF AC.

9.13. Disposiciones de resolución de disputas
Según lo definido en la DPC de ANF AC.

9.14. Ley aplicable
Según lo definido en la DPC de ANF AC.

9.15. Cumplimiento de la legislación aplicable

Según lo definido en la DPC de ANF AC.

9.16. Otras disposiciones

Según lo definido en la DPC de ANF AC.

9.17. Otras provisiones

Ninguna estipulación.